New Approaches to Suzuki's CA-Proof

A Thesis Presented
by
Elizabeth Wilcox
to
The Faculty of the Graduate College
of
The University of Vermont

In Partial Fulfillment of the Requirements
for the Degree of Master of Science
Speciailizing in Mathematics

May, 2008

Abstract

Many real world and mathematical objects exhibit symmetries, which can be successively combined (or "multiplied") to create new symmetries. This law of "multiplication" led to the formulation of abstract structures known as *groups*, and the study of group theory has become a main branch in modern mathematics.

A fundamental result in group theory is that groups containing only a finite number of elements can be "uniquely factored," similar to the unique factorization of integers, with so-called *simple groups* being the analog of prime numbers.

One of the major mathematical results in the last century was the determination of the complete list of all finite simple groups: the *Classification of Finite Simple Groups*. This Theorem, in its original form, requires some 15,000 journal pages spanning about 500 articles by more than 100 mathematicians (written mostly between 1940 and 1980).

A cornerstone of this Classification is a famous paper by Michio Suzuki on so-called CA-groups. Our work is an attempt to shed new light on the pivotal CA-group proof, at least in special cases, by using different techniques than Suzuki, such as methods from permutation group theory and graph theory.

Acknowledgements

There are many to whom I owe deep gratitude – beginning with my family and friends, especially my parents and Jonah. Without the academic inspiration provided by Dr. Deanna Haunsperger of Carleton College and then by Dr. Jonathan Sands of the University of Vermont, I am sure that mathematics and algebra would not be my path. I am deeply indebted to my advisor, Dr. Richard Foote, who deserves many a gold star for patience, eagerness, and persistence.

Thank you.

Contents

List of Tables

List of Figures

Introduction

"It has been seen that there is in some respects a marked difference between groups of even and those of odd order. ... The contrast that these results shew between groups of odd and of even order suggests inevitably that simple groups of odd order do not exist."

These sentences were first published in Note M of William Burnside's text "Theory of Groups of Finite Order" in 1898 [2]. It wasn't until 1962 that Walter Feit and John Thompson proved this conjecture of Burnside. It subsequently became part of the Classification of Finite Simple Groups. This classification provides a complete list of all finite simple groups, one of the major mathematical results in the last century. The Feit-Thompson proof of this conjecture of Burnside was a crucial step in the classification process, which is the combined work of over 100 mathematicians distributed over more than 500 journal articles. Feit and Thompson's proof alone took over 255 pages – an entire journal issue [6].

By 1900 Burnside had made some progress towards the proof of his conjecture, demonstrating that groups of odd order less than 40,000 must be solvable. Burnside's method of proof involved investigation on a case-by-case strategy. It wasn't until 1957 that a major stepping stone toward the proof of the Feit-Thompson Theorem and the Classification was accomplished by Michio Suzuki's proof of the following theorem (on which they both rely) [11].

Theorem 0.0.1 (Suzuki's Theorem)**.** *Every odd order CA-group is solvable.*

A *CA-group* is a non-abelian group wherein the centralizer of every nonidentity element is abelian. In other words, if y and z are elements of a CA-group that commute with a third element $x \neq 1$ then y and z must also commute with one another. It turns out that CA-groups tend to appear in "minimal situations," since they possess configurations that satisfy the Class Equation as a hypothetical simple group of the same order would. Burnside encountered one of order $3^3 \cdot 7 \cdot 13 \cdot 409$ in his work, and this group is the *only* one with order less than $40,000$ that he couldn't show solvable by elementary means alone. We call the order of such a possible simple group a *Burnside number*; and through the course of this research we identified a new Burnside number $3^7 \cdot 13 \cdot 41 \cdot 547 \cdot 1093 \cdot 4493$. We have also developed a group theoretic proof to show that such a group must be solvable. Burnside turned to character theory to prove that a CA-group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ must be solvable, though we present here a proof using permutation group theory.

Part of the reason why solvability of odd order CA-groups is difficult to show is that simple even order CA-groups do exist. However, the structure of hypothetical odd order simple CA-groups is so close to that of simple even order CA-groups that traditional counting arguments of group theory did not seem to provide an overarching proof of solvability – despite the fact that one can often show using elementary group-theoretic techniques alone that a *particular* odd order CA-group is solvable. For this reason, Suzuki followed Burnside's lead and turned to character theory for his proof.

Since the publication of Suzuki's Theorem and then that of Feit and Thompson's Theorem, mathematicians have been attempting to streamline the entire Classification; but to the best of our knowledge no fundamental new insights have been achieved for simplifying Suzuki's paper. Simplifying this particular step in the Classification could have a ripple effect, not only by introducing new techniques to examine groups but also because Suzuki's Theorem is directly quoted in the proof of the Feit-Thompson Theorem. An article by R. Solomon [Solomon] quotes Thompson as writing "Suzuki's CA-theorem is a marvel of cunning … Once one accepts this theorem as a step in a general proof, one seems irresistibly drawn along the path which was followed [in the Odd Order Paper]." So one sees that the CA-theorem is not only brilliant for its own sake, but also for the direction it gave other group theorists in continuing the work of the Classification. Our work in this thesis is an attempt to shed new light on the pivotal CA-group proof, at least in special cases, by using different techniques than Suzuki, such as methods from permutation group theory and graph theory. We hope that a new method of proof for even a part of the CA-theorem can give further insight into the other steps in the Classification, in particular the proof of Feit and Thompson's Theorem.

We begin in Chapter 1 with the definitions and theorems needed to understand the structure of CA-groups and their Frobenius subgroups. Definition and discussion of TI-sets and Frobenius groups involves the pertinent group theory as well as character theory. In this chapter, the definition of CA-groups is revisited in detail and consequences of this definition are developed. Primary examples of CA-groups are introduced, including the familiar alternating group on five points, A_5. Chapter 2 elaborates on Burnside's approach, introducing in greater depth the difficulty in showing that a CA-group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ is solvable. This chapter also provides an outline of the proof of Suzuki's Theorem and discusses some of the details in relation to A_5. Chapter 3 begins to describe our original work, which focuses on simple CA-groups of order $p^a qr$ having three conjugacy classes of Frobenius subgroups. Our approach is to first eliminate the cases of odd order simple CA-groups with one or two conjugacy classes of Frobenius subgroups, then generalize to CA-groups with three conjugacy classes of Frobenius subgroups. In some special instances we deal with CA-groups having four such classes to illustrate certain concepts or techniques. We provide in this chapter a permutation-group-theoretic proof that there are no simple odd order CA-groups of order $p^a qr$ where the Sylow p-subgroup is elementary abelian. We also define a collection of graphs associated with a group and explore the consequences these graphs have on the existence of a group. In this chapter we present an alternate proof that a CA-group of order $p^a qr$ with an elementary abelian Sylow p-subgroup is solvable using graph theory. Finally, we conclude by discussing the progress that our efforts have produced, the shortcomings of our methods, and what directions remain to be explored, as we have not yet cracked the general case of Suzuki's proof.

The reader should note that unless otherwise noted explicitly, the term “group” will mean “finite group.” We expect the reader is familiar with the notation and results in Parts I and VI of [4], regarding group theory and character theory.

Chapter 1

CA-Groups and Their Frobenius Subgroups

In this chapter we present the background information regarding the structure and character theory of CA-groups. We first begin by introducing TI-sets and Frobenius groups, including the related character theory. Every CA-group contains at least one Frobenius subgroup, and it is through the interactions of these subgroups with one another that an odd order CA-group can be shown solvable. Thus a thorough understanding of the structure and properties of Frobenius groups is crucial for understanding that of CA-groups.

Before continuing though, we present without proof two results of Schur that are used in the chapter.

Theorem 1.0.2. *[7, Theorem 3.5.3 (Schur's Lemma)] Let q and p be distinct primes and let A be any noncyclic abelian q-group such that A acts as automorphisms on a p-group, P. Then*

$$P = \langle C_P(x) \mid x \neq 1 \textit{ and } x \in A \rangle.$$

Theorem 1.0.3. *[4, Theorem 17.39 (Schur's Theorem)] If G is any finite group containing a normal subgroup whose order is relatively prime to its index (i.e., a π-Hall subgroup), then there exists a complement to the normal subgroup in G.*

Some notation needs to be specified. Throughout this work we will be using exponential notation to denote conjugation, so that for any element g in a group

G

$$H^g = g^{-1}Hg \text{ and } x^g = g^{-1}xg$$

where $H \leq G$ and $x \in G$.

Additionally, for the class functions ψ and φ of a group G, the term *inner product (with respect to G)*, denoted $(\psi, \varphi)_G$, is used to represent the following formula:

$$(\psi, \varphi)_G = \frac{1}{|G|} \sum_{g \in G} \psi(g)\overline{\varphi(g)}.$$

The inner product of ψ with itself is shortened to $||\psi||^2$. We use ρ_G to represent the regular character of a group (or subgroup) G. Typical notation to represent the character ψ induced from a subgroup H up to a group G is $\mathrm{Ind}_H^G(\psi)$. The formula for induction is given by:

$$\mathrm{Ind}_H^G(\psi)(x) = \frac{1}{|H|} \sum_{x \in G} \psi(x^{-1}gx),$$

where ψ is extended by making it zero on $G - H$. Often we will have $K \leq H \leq G$ and will be inducing characters of K up to either H or G. To shorten the notation but still provide a distinction, we shall write $\mathrm{Ind}_H^G(\psi) = \psi^*$ and $\mathrm{Ind}_K^H(\psi) = \widetilde{\psi}$ so that an asterisk always indicates induction to the whole group G. Recall that by Frobenius Reciprocity [5, Theorem 1.9.4], if $H \leq G$ with ψ a character of H and φ a character of G then

$$(\psi^*, \varphi)_G = (\psi, \varphi_{|H})_H.$$

1.1 Frobenius Groups

The information provided here has been restricted to facts pertinent to the solvability of all odd order CA-groups, though more of the group theory involved in Frobenius groups has been unraveled. For further information about these groups, a reader should refer to [13].

Definition 1.1.1. A non-abelian group G is a *Frobenius group with Frobenius kernel* K if and only if there exists a proper nontrivial $K \trianglelefteq G$ such that $C_G(x) \leq K$ for every nonidentity $x \in K$.

Frobenius groups have a very rigid structure leading to properties that hold regardless of the order of the group. One such characteristic is that every Frobenius group has a set of TI-subgroups known as the Frobenius complements.

Definition 1.1.2. A subset $H \leq G$ is called a *trivial intersection subset*, or *TI-subset*, if $H \cap H^g \subseteq \{1\}$ for every $g \in G - N_G(H)$. In particular, if the TI-subset H is a subgroup of G then H is called a *TI-subgroup.*

The definition implies that every normal subgroup is a TI-subgroup, since $G - N_G(H)$ is empty for $H \trianglelefteq G$. Subgroups of prime order are always TI-subgroups. A nontrivial TI-set would be the Klein-4 group as a subset of A_5. In A_4, the group $V_4 = \langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is normal and indeed $N_{A_5}(V_4) = A_4$; but $A_4 \leq A_5$. Calculations in A_5 show that this V_4 subgroup is a TI-subgroup of A_5. Proposition 1.1.3 below introduces a useful property of TI-sets.

Proposition 1.1.3. *Let A be a TI-set contained in a group G and let $a \in A$ be an element other than the identity. For $g \in G$ the element $g^{-1}ag \in A$ if and only if $g \in N_G(A)$.*

Proof. The reverse direction is by definition of the normalizer of A. To prove the forward direction, consider $g \in C_G(a)$. Then $g^{-1}ag = b \in A$ so $b \in A^g \cap A$. By definition of TI-set, $g \in N_G(A)$. ■

Note that Proposition 1.1.3 implies $C_G(a) \leq N_G(A)$ for every nonidentity $a \in A$. This proposition can be used as an alternate definition of TI-set.

That Frobenius groups contain TI-subgroups is important for defining their overall structure. Summarized in Lemma 1.1.4 are the properties of Frobenius subgroups pertinent to our discussion.

Lemma 1.1.4. *Given G a Frobenius group with Frobenius kernel K, the following holds:*

1. *K is a π-Hall subgroup.*
2. *There exists a complement to K in G, E, such that E is a TI-subgroup, $G = KE$, and $N_G(E) = E$.*

3. *If $|E|$ is even, then K is abelian.*

4. *(Thompson) K is nilpotent.*

5. *For every nonidentity $g \in E$, g acts fixed-point free by conjugation on the nonidentity elements of K.*

6. *All complements to K in G are conjugate in G.*

7. *Every element of G lies either in K or some conjugate of E.*

Proof. Parts (3) and (4) of this theorem are proved in [9, Proposition 8.3] and [5, Theorem 25.8], respectively. Part (5) is an easy exercise. Here we prove the remaining parts.

To show part (1), let $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $\alpha_i \in \mathbb{N}$ for every i and $p_i^{\alpha_i}$, $p_j^{\alpha_j}$ are distinct primes for $i \neq j$. Let $p_i \bigm| |K|$. We will show that $p_i^{\alpha_i}$ divides the order of K. Let $p_i = p$, and $P_0 \in \mathrm{Syl}_p(K)$. Then P_0 is a subgroup of P for some $P \in \mathrm{Syl}_p(G)$. Suppose $P_0 \neq P$ (*i.e.*, suppose the full power of p does not divide $|K|$). If we let $P_1 = N_P(P_0)$, then P_0 is a proper subgroup of P_1 by virtue of their both being p-groups [4, Theorem 6.1]. This same theorem implies that $P_0 \cap Z(P_1) \neq 1$. Let x be a nonidentity element in the intersection of P_0 and $Z(P_1)$. Then $P_1 \leq C_G(x)$ but by definition of Frobenius kernel, $C_G(x) \leq K$. Therefore $P_1 \leq K$, which contradicts the assumption that P_0 is a Sylow p-subgroup of K. Thus $P_0 = P \in \mathrm{Syl}_p(G)$ and K is a π-Hall subgroup of G.

By Theorem 1.0.3, Schur's Theorem, there exists a complement to K in G. Let that complement be E. By definition of complement $G = KE$. For every nonidentity element $a \in E$, we have that $C_G(a) \leq E$. If not, then because $G = KE$ we would have $C_G(a) \cap K \neq 1$, so there exists a nonidentity element $x \in K$ such that $ax = xa$. Therefore $a \in C_G(x) \leq K$, and $a \in K$, which contradicts the fact that $K \cap E = 1$. Thus E is a TI-subgroup of G, complement to K.

To prove that $N_G(E) = E$, let $x \in N_G(E) \leq G$. As $G = KE$, there exists $k \in K$ and $e \in E$ such that $x = ke$. As $x = ke$ normalizes E, we also have

$k \in N_G(E)$. Consider then $[k, E]$. Since k normalizes E, we have $[k, E] \leq E$ but E normalizes K so $[k, E] \leq K$. Therefore $[k, E] \leq E \cap K = 1$, implying k centralizes E. Since $C_G(E) \leq E$, $k = 1$ and $x = e \in E$. Therefore $N_G(E) = E$.

This establishes parts (1) and (2) of the lemma. Let E' be a second complement to K in G. Then $G = KE'$ and so $G/K \cong E'$, by definition of complement. Thus $E \cong E'$, and they are both π-Hall subgroups of G for the same set π. Therefore, by [4, Exercise 6.1.33], E and E' are conjugate in G. (This exercise assumes G is solvable, but it requires only that K be solvable, which is true by (4).) Thus (6) is established and (7) easily follows by counting elements in conjugates of E. ■

There are many familiar examples of Frobenius groups. The nonabelian group of order pq where p and q are primes with $q \mid (p-1)$ is a Frobenius group. In such a group, G, if we let P and Q be the Sylow p- and q-subgroups of G (respectively) then both are cyclic but P is normal in G and Q is not. Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. Since G is non-abelian x and y do not commute and so $C_G(x) \leq P$. As x was any generator of P, G is Frobenius. (Here $K = P$ and $E = Q$ in our previous notation.)

A second familiar example of a Frobenius group is the dihedral group of order $2n$ for n odd, denoted D_{2n}. In this group the Frobenius kernel is the cyclic group of order n, $\langle r \rangle$, and a Frobenius complement is $\langle s \rangle$ where s is any reflection. Note that for every $k \in \mathbb{N}$ such that $r^k \neq 1$ the centralizer of r^k is equal to $\langle r \rangle$ because s inverts r^k and $r^{-k} \neq r^k$ where $|r|$ is odd. (If n is even, D_{2n} is not a Frobenius group because $r^{n/2}$ commutes with s.)

There are also examples among the symmetric and alternating groups. Since $S_3 \cong D_6$ we see already that S_3 is a Frobenius group. As mentioned earlier, the alternating group A_4 has a normal Sylow 2-subgroup V_4 whose elements are represented by products of two commuting 2-cycles. An element of V_4 commutes only with itself and the identity. Therefore V_4 is the Frobenius kernel and a Frobenius complement E is a group generated by a 3-cycle (which is self-normalizing and TI, by Sylow's Theorem).

We will be considering how Frobenius groups act on sets in Chapter 3. To this end, we introduce Definition 1.1.5.

Definition 1.1.5. Let G act transitively as permutations on a set Ω. A normal subgroup N of G is called a *regular normal subgroup* if N is transitive on Ω and the identity is the only element of N that fixes any point in Ω.

If G is a Frobenius group with Frobenius kernel K and complement E, let Ω be the set of conjugates of E so that G acts transitively by conjugation on Ω. Then K is a regular normal subgroup of G with respect to this action. The following proposition may be found in [9, Proposition 4.2].

Proposition 1.1.6. *Let G be a permutation group acting on a set Ω, and let K be a regular normal subgroup of G. For $\alpha \in \Omega$ the action of G_α on $\Omega - \{\alpha\}$ is the same (i.e., permutation isomorphic) as the action of G on $K - 1$ by conjugation.*

Proposition 1.1.6 dictates the behavior of any Frobenius complement in regards to a set upon which G acts transitively. That behavior is laid out in Corollary 1.1.7, below.

Corollary 1.1.7. *Let $G = KE$ be a Frobenius group with Frobenius kernel K such that G acts transitively on a set Ω and K is a regular normal subgroup for this action. Then E fixes one point in Ω.*

Proof. The normal subgroup K is regular, so by Proposition 1.1.6 the action of G_α on $\Omega - \{\alpha\}$ is the same as the action of G on $K - 1$ by conjugation. For some $\alpha \in \Omega$, we have that G_α is a complement to K in G, so by Lemma 1.1.4 (7) we may choose α so that $G_\alpha = E$. The action of G_α is now equivalent to the action of E on $K - 1$ by Proposition 1.1.6. We know that E acting by conjugation on K fixes only the identity in K, so E fixes only α in Ω. ∎

In addition to the structure and group theory of Frobenius groups being well established, the character theory of Frobenius groups is also known. Proposition 1.1.8, whose proof can be generalized from one found in [4, Proposition 19.3], and Corollary 1.1.9 describe the complete set of nonprincipal irreducible characters of a Frobenius group.

Proposition 1.1.8. *Let G be a Frobenius group with Frobenius kernel K. If χ is an irreducible character of G without K in its kernel, then there exists a non-principal irreducible character ζ of K such that $\zeta^* = \chi$.*

Note that by the formula for character induction, every nonprincipal irreducible character of the Frobenius group G either has K in its kernel or is zero on all elements of $G - K$. The following corollary is an immediate consequence of Proposition 1.1.8, and determines every character of certain Frobenius groups.

Corollary 1.1.9. *Let $G = KE$ be a Frobenius group with Frobenius kernel K and complement E such that $|K| = k$ and $|E| = e$. Assume both K and E are abelian. Then G has exactly $\frac{k-1}{e}$ irreducible characters of degree equal to $|G : K|$, and e characters of degree 1 (all with K in their kernel). These account for all irreducible characters of G.*

We have thus determined the character table for any Frobenius group G that we will encounter in this thesis. The character table of D_{10} for instance includes exactly $\frac{5-1}{2} = 2$ irreducible characters of degree $|G : K| = 2$ and 2 degree 1 characters, each with $\langle r \rangle$ in its kernel. The irreducible degree 1 characters (including the principal character of D_{10}) are the irreducible characters of $D_{10}/\langle r \rangle \cong Z_2$. As the degree 2 characters are induced from the normal subgroup $K = \langle r \rangle$, by the formula for induction these characters must be zero on the conjugacy class of s. The degree 2 characters take the value of a sum of 5^{th} roots of unity on each of the remaining conjugacy classes and after consideration, there are only two distinct possibilities for those values which we represent with ξ and ξ^*. Let $\zeta = e^{2\pi i/5}$, then its conjugate is $\overline{\zeta} = e^{-2\pi i/5}$. Thus $\zeta + \overline{\zeta} = \frac{-1+\sqrt{5}}{2} = \xi$ and $\zeta^2 + \overline{\zeta^2} = \frac{-1-\sqrt{5}}{2} = \xi^*$. The finished character table is presented in Table 1.1 for inspection.

Frobenius provided another characterization of Frobenius groups using the fact that the Frobenius complement is a TI-subgroup. This characterization relies on a proposition about class functions.

Definition 1.1.10. A *class function* is a function from a group G into a field F that is constant on the conjugacy classes of G.

classes:	1	r	r^2	s
sizes:	1	2	2	5
1	1	1	1	1
χ_1	1	1	1	-1
χ_2	2	ξ	ξ^*	0
χ_3	2	ξ^*	ξ	0

Table 1.1: The character table of D_{10}.

Any function from an abelian group into a field is trivially a class function, as the conjugacy classes of an abelian group are composed of single elements. Characters are nontrivial class functions. Using characters as a model, we can also generalize the concept of induction to class functions.

Definition 1.1.11. If θ is any class function on a subgroup H of a larger group G, define the *induction of θ to G* by

$$\theta^*(x) = \frac{1}{|H|} \sum_{g \in G} \theta(g^{-1}xg)$$

where θ is extended to be zero on $G - H$.

We now present a proposition about class functions that will ultimately allow us to finally give Frobenius' characterization of Frobenius groups.

Proposition 1.1.12. *Let A be a TI-subgroup in a group G with $N = N_G(A)$. Let α and β be class functions on N such that $\alpha = 0$ on $N - A$ and $\beta(x) = 0$ whenever $x \in N - A$ and x is a conjugate in G to some element of A. Then:*

1. *$\alpha^*(a) = \alpha(a)$ and $\beta^*(a) = \beta(a)$ for every nonidentity $a \in A$, and*
2. *if $\alpha(1) = 0$ then $(\alpha^*, \beta^*)_G = (\alpha, \beta)_N$.*

Proof. To prove part (1) of the proposition, consider the definition of α^* on a nonidentity element $a \in A$.

$$\begin{aligned}
\alpha^*(a) =& \frac{1}{|N|}\sum_{g\in G}\alpha(g^{-1}ag) \\
=& \frac{1}{|N|}\sum_{g\in N}\alpha(g^{-1}ag) \quad \text{since } \alpha(g)=0 \text{ for } g\in G-N_G(A) \\
=& \frac{1}{|N|}|N|\alpha(a) \quad \text{by definition of class function on } N \\
=& \alpha(a).
\end{aligned}$$

Similarly, $\beta^*(a) = a$ for all nonidentity $a \in A$. A proof of the second part relies on the definition of inner product. Since α^* is zero outside conjugates of A and $\alpha^*(1) = 0$, we can reduce to:

$$\begin{aligned}
(\alpha^*, \beta^*)_G =& \frac{1}{|G|}\sum_{g\in G}\alpha^*(g)\overline{\beta^*(g)} \\
=& \frac{1}{|G|}\frac{|G|}{|N|}\sum_{g\in A}\alpha^*(g)\overline{\beta^*(g)} \quad \text{as there are } |G:N| \text{ conjugates of } A, \\
=& \frac{1}{|N|}\sum_{g\in A}\alpha(g)\overline{\beta(g)} \quad \text{by part (1).}
\end{aligned}$$

Thus both parts of the proposition are shown. ■

Note that the hypotheses on β, which seem to have the potential to be constraining, hold automatically when the subgroup A is TI in G with β equal to zero on $N - A$ and $|N : A|$ relatively prime to $|A|$. In other words, if A is a π-Hall subgroup of G with the class function β zero on $N - A$ then the hypotheses of Proposition 1.1.12 hold. We are now ready to present a method of characterizing Frobenius groups developed by Frobenius himself.

Theorem 1.1.13 (Frobenius)**.** *If the group G has a proper TI-subgroup E such that $N_G(E) = E$, then E has a normal complement K in G, and G is a Frobenius group with Frobenius kernel K and complement E.*

Proof. We first construct the normal complement to E, and call it K. Let $\{\zeta_i\}$ be the set of nonprincipal irreducible characters of E and define $\alpha_i = \zeta_i(1)1_E - \zeta_i$, where 1_E is the principal character of E. Then α_i is a class function on E and $\alpha_i(1) = 0$. By Proposition 1.1.12,

$$||\alpha_i^*||^2 = \zeta_i(1)^2 + 1.$$

By Frobenius Reciprocity we then have $(\alpha_i^*, 1_G)_G = (\alpha_i, 1_E)_E = \zeta_i(1)$. Since $\alpha_i(1) = 0$, we must have $\alpha^* = \zeta_i(1)1_G - \chi_i$ for some irreducible character χ_i of G of degree $\zeta_i(1)$.

Let $g \in G$ not be conjugate to any element of E. Then $\alpha_i^*(g) = 0$ for every i. This implies that for every i we have $\zeta_i(1)1_G(g) - \chi_i(g) = 0$. Therefore $\chi_i(g) = \zeta_i(1) = \chi_i(1)$, and so g is in the kernel of χ_i. Thus there exists a subgroup K_i which is the kernel of χ_i. This subgroup is nontrivial as $g \in K_i$ and g is not conjugate to any element in E. Define the normal subgroup K by

$$K = \bigcap_i K_i.$$

By the above, $K \trianglelefteq G$ and $g \in K$. We now show that $G = KE$ by defining a character θ, that we will ultimately show is $\rho_{G/K}$. Define θ by

$$\theta = 1_G + \sum_i \chi_i(1)\chi_i.$$

For any $g \in K$, the value $\theta(g)$ is given by

$$\begin{aligned}\theta(g) &= 1 + \sum_i \chi_i(1)\chi_i(g)\\ &= 1 + \sum_i \chi_i(1)^2\\ &= 1 + \sum_i \zeta_i(1)^2\\ &= \rho_E(1)\\ &= |E|\end{aligned}$$

and note that $\theta(g) = \theta(1)$. We will show that if $h \notin K$ then $\theta(h) = 0$. By construction, if $g \in G - K$ then g is in the union of the conjugates of E. So the elements of E are representatives of the conjugacy classes in $G - K$ and therefore if the value of θ is zero on every nonidentity element $h \in E$, then θ is zero on every element $h \notin K$. Let $E^\sharp = E - \{1\}$. On $E^\sharp$, the class function $\alpha_i^* = \alpha_i$. Recall that by definition we have

$$\begin{aligned}\alpha_i &= \zeta_i(1)1_E - \zeta_i \quad \text{and}\\ \alpha_i^* &= \zeta_i(1)1_G - \chi_i.\end{aligned}$$

This means that for every $h \in E^\sharp$, we have that $\zeta_i(1) - \zeta_i(h) = \zeta_i(1) = \chi_i(h)$ which implies that $\zeta_i(h) = \chi_i(h)$. Thus, the value of θ on h can be determined:

$$\begin{aligned}\theta(h) &= 1 + \sum_i \chi_i(1)\chi_i(h)\\ &= 1 + \sum_i \zeta_i(1)\zeta_i(h)\\ &= \rho_E(h)\\ &= 0.\end{aligned}$$

We have therefore shown that θ is actually ρ_E on E. If in fact, $\theta = \rho_{G/K}$, then $G/K = E$, so $|G/K| = |E|$ and $K \cap E = \{1\}$ will imply $G = KE$, as needed.

Let $\overline{G} = G/K$. Any character which is zero on all nonidentity elements of a group is a multiple of the group's regular representation. Therefore, $\theta = m\rho_{\overline{G}}$ for some integer $m > 0$. We also know that by definition θ is a character of $\overline{G}$, since the χ_i all have K in their kernels.

Consider the definition of θ and that of $\rho_{\overline{G}}$, which is the same sum but over all irreducible characters of $\overline{G}$. So $\rho_{\overline{G}}$ has at least as many components as θ and perhaps more. Let $\alpha = \rho_{\overline{G}} - \theta$. Either α is identically zero or it's a character of $\overline{G}$, depending whether or not $\alpha(\overline{1})$ is zero since α is zero on all other elements of $\overline{G}$.

The class function α has no copies of the principal character, since both $\rho_{\overline{G}}$ and θ have exactly 1 copy each. Evaluate the inner product of α and $1_{\overline{G}}$. The inner product can only be zero if the degree of α is zero, since the degree must be a nonnegative real number. This implies then that α is identically zero, and $\theta = \rho_{\overline{G}}$. This completes the proof. ∎

The proof of Theorem 1.1.13 provides an alternate way of identifying Frobenius groups. The theorems and propositions of this section by no means present the entire picture of Frobenius groups. However, the information provided here is the necessary background for understanding the structure of CA-groups, which we begin to unravel in the following section.

1.2 CA-Groups

In the introduction we defined the term CA-group. This definition was:

Definition 1.2.1. A non-abelian group G is called a *CA-group* if and only if the centralizer of every nonidentity element in G is abelian.

Let us consider some examples of CA-groups. The most familiar examples are non-abelian groups of order pq, dihedral groups D_{2n} for n odd, A_4, and the simple group A_5 which has order $2^2 \cdot 3 \cdot 5$. The elements of $G = A_5$ are 3-cycles, 5-cycles, and products of two commuting 2-cycles. A 3-cycle $(a\ b\ c)$ only commutes in S_5 with elements that are products of its own powers and permutations whose entries are distinct from a, b, and c. For instance, the permutation $(1\ 2\ 3)$ commutes with its own powers and $(4\ 5)$, however the latter permutation is not actually an element of A_5. Thus $(1\ 2\ 3)$ and the other 3-cycles in A_5 commute only with their own powers and for $(a\ b\ c) \in A_5$, we have that $C_G((a\ b\ c)) = \langle (a\ b\ c) \rangle$. A similar situation occurs with the 5-cycle elements. What remains to be shown is that permutations such as $(1\ 2)(3\ 4)$ have abelian centralizers. Unlike the permutations that have exactly one cycle in their decomposition, an element $(a\,b)(c\,d)$ commutes with other "two 2-cycles" provided they both fix the same point in $\{1, 2, 3, 4, 5\}$. So $(1\ 2)(3\ 4)$ commutes with $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$ but not with an element that permutes 5, like $(1\ 5)(2\ 3)$. In the case of the "two 2-cycles," $C_G((a\,b)(c\,d)) = \{(1), (a\ b)(c\ d), (a\ c)(b\ d), (a\ d)(b\ c)\}$. The centralizer of any nonidentity element in that subgroup is the same, thus $C_G((a\ b)(c\ d))$ is abelian, and A_5 satisfies the definition of being a CA-group.

Proposition 1.2.2, below, lays out the general properties of a CA-group.

Proposition 1.2.2. *Let G be a CA-group. Then*

1. *All subgroups of G are also CA or abelian.*
2. *If x is a nonidentity element of G then $C_G(x) \leq C_G(x^n)$ for all $n \in \mathbb{Z}$.*
3. *All Sylow subgroups of G are abelian and TI.*
4. *Let $N \trianglelefteq G$ and denote G/N with $\overline{G}$. If the prime p does not divide $|N|$ then for every $x \in G$ such that $|x| = p$, $C_{\overline{G}}(\overline{x}) = \overline{C_G(x)}$.*
5. *The homomorphic image G/N of a CA-group is either abelian or a CA-group when $N \trianglelefteq G$ and $|N| = q^b$ for a prime q.*
6. *If G is CA and N is solvable, then G/N is CA or abelian.*

Proof. The proof of parts (1) and (2) are obvious, and part (4) appears as an exercise in [4, Section 6.1]. We present proofs of the remaining parts of the proposition.

To show part (3), let P be a Sylow p-subgroup of G for a prime p dividing $|G|$. Since P is a p-group its center is nontrivial. Let x be a nonidentity element of $Z(P)$. Then $C_G(x)$ is abelian, but as $x \in Z(P)$ we have that $P \leq C_G(x)$. Therefore P is abelian. Let y be a nonidentity element in $P \cap P^g$ for $g \in G$. Both P and P^g are subgroups of $C_G(y)$, which is abelian. Therefore P and P^g are Sylow subgroups of $C_G(y)$ so both are normal in $C_G(y)$ and thus equal. We then have that if $P \neq P^g$, their intersection is exactly 1. Therefore the Sylow subgroups are TI.

For part (5) first note that for $x \in G$ if $|x| = p \neq q$ then by (4) $C_{\overline{G}}(x) = \overline{C_G(x)}$. Since $C_G(x)$ is abelian, $\overline{C_G(x)}$ is abelian. If $|x| = p = q$, let $H = \langle x, N \rangle$, which is a q-subgroup in G. Then there exists a $Q \in \mathrm{Syl}_q(G)$ such that $H \leq Q$, therefore H is abelian. Let $\overline{K} = C_{\overline{G}}(\overline{x})$ and K be the complete preimage of $\overline{K}$ under the usual projection map from G to $\overline{G}$. Then by the Lattice Isomorphism Theorem, $H \trianglelefteq K$.

We now show that $H \leq Z(K)$. Let y be a nonidentity element of K; we may assume that $|y|$ is the power of a prime. If not, $|y| = r_1^{\alpha_1} r_2^{\alpha_2} \cdots r_n^{\alpha_n}$ where r_i is a prime and $n \in \mathbb{N}$. In this case $y = y_1 y_2 \cdots y_3$ where $|y_i|$ is the power of a prime. If y doesn't commute with H, some y_i doesn't commute with H so our assumption generalizes. Therefore let $|y| = r^\alpha$. If $r = p = q$ then $\langle H, y\rangle$ will be a q-group and therefore abelian. If r is not equal to $p = q$ then the Fitting Lemma [7, Theorem 5.2.6] asserts $H = C_H(y) \times [H, y]$.

We argue that the subgroup $C_H(y) \neq 1$. If true then there exists some non-identity $z \in C_H(y)$ such that $[H, y] \leq C_G(z)$, which implies that y commutes with H as desired, and so $H \leq Z(K)$, so $H = K$. We see then that K is abelian and therefore $\overline{K}$ is abelian. We thus need only show that $C_H(y) \neq 1$, which we prove by contradiction. Assume that $C_H(y) = 1$, then $H = [H, y]$ and $\overline{H} = [\overline{H}, y]$. However $\overline{H} = H/N = \langle x, N\rangle/N = \langle \overline{x}\rangle$. By definition of K we have $\langle \overline{x}\rangle \leq Z(\overline{K})$, so $[\overline{H}, y] = \overline{1} \neq \overline{H}$. This establishes (5).

For the last part of the proposition note that N is solvable so there exists a subgroup $A \trianglelefteq N$ such that $A \trianglelefteq G$ and $|A| = q^b$ for some prime q and some $b > 0$. Then by part (5), G/A is a CA-group. Using induction, all of N may be factored to show that $\overline{G}/\overline{N}$ is CA. By the Isomorphism Theorems, $A \trianglelefteq G$ implies that $\overline{G}/\overline{N} \cong G/N$. Therefore G/N is CA as well. ■

The main consequence of Proposition 1.2.2 is that when one attempts to prove that some family of CA-groups (such as odd order CA-groups) are solvable one needs only work with a counterexample of minimal order. In such a group, by induction the proper subgroups are CA and solvable, so if there exists $N \trianglelefteq G$ then G/N is CA and of smaller order than G, thus is solvable. For this reason, we begin every proof of the solvability of particular CA-groups by considering a counterexample of minimal order which then is seen to have no proper nontrivial normal subgroups, *i.e.*, is a simple group. We call such counterexamples *minimal simple CA-groups*. Unless specified in the proof, we do not assume a particular parity to the group order since minimal simple CA-groups of even order *do* exist. (e.g., A_5, $\mathrm{SL}_2(2^p)$ for a prime p).

As promised, the connection between Frobenius groups and CA-groups becomes obvious under the next proposition.

Proposition 1.2.3. *Let G be a simple CA-group and K be a maximal abelian subgroup of G. Then K is a π-Hall subgroup of G with $N_G(K) = KE$ a Frobenius group with Frobenius kernel K and complement E for some $E \leq G$. Furthermore, K is a TI subgroup of G.*

Proof. We will proceed with this proof in steps. First, we will show that K is a TI-set and a π-Hall subgroup. Second, we will show that $N_G(K)$ is a Frobenius group.

To begin, consider $t \in G$ such that $K \cap K^t \neq 1$. Let x be a nonidentity element in $K \cap K^t$. Then $C_G(x)$ must contain both K and K^t, since both are abelian. Thus $K \leq C_G(x)$, but K is a maximal abelian subgroup of G so $C_G(x) = K$. By similar argument, $C_G(x) = K^t$. Therefore $K = K^t$, and so K is TI in G.

If K is not a π-Hall subgroup of G, there exists prime p dividing the order of G with $P_0 \in \mathrm{Syl}_p(K)$ and $P \in \mathrm{Syl}_p(G)$ such that $P_0 < P$. Let $P_1 = N_P(P_0)$. Since these are p-groups and $P_0 \trianglelefteq P_1$, we have that $P_0 \cap Z(P_1) \neq 1$. Let x be a nonidentity element in this intersection. From the last paragraph we know that $C_G(x) = K$ therefore $P_1 \leq K$, which contradicts the fact that $P_0 \in \mathrm{Syl}_p(K)$. Therefore $P_0 = P$ and K is a π-Hall subgroup.

We next show that $N_G(K)$ is a Frobenius group. Clearly $K \trianglelefteq N_G(K)$, and K is a Hall subgroup of N. Every nonidentity $x \in K$ has $K \leq C_G(x)$, but K is a maximal abelian subgroup of G, therefore $K = C_G(x)$. Thus $N_G(K)$ is a Frobenius group. The remainder of the proposition follows from Lemma 1.1.4. ∎

Thus in any simple CA-group the maximal abelian subgroups of G form the kernels of Frobenius subgroups which are their normalizers. Such subgroups are CA by Proposition 1.2.2, with normal abelian subgroups that are solvable. In the explanation of how A_5 satisfies the definition of CA-group; it was shown that $P = C_G((1\ 2)(2\ 3))$ is an abelian subgroup of order 4 (therefore is a Sylow 2-subgroup) and that its elements did not commute with other "two 2-cycles." It was also shown that 3-cycles and 5-cycles commute only with their own powers; thus P is a maximal abelian subgroup. This also results in maximal abelian subgroups $Q = \langle(1\ 2\ 3)\rangle$ and $R = \langle(1\ 2\ 3\ 4\ 5)\rangle$ (also Sylow subgroups, associated with the

Sylow Prime	Kernel (K)	Complement (E)	$N_G(K) = KE$
2	$\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$	$\langle(2\ 3\ 4)\rangle$	A_4
3	$\langle(1\ 2\ 3)\rangle$	$\langle(2\ 3)(4\ 5)\rangle$	S_3
5	$\langle(1\ 2\ 3\ 4\ 5)\rangle$	$\langle(2\ 5)(3\ 4)\rangle$	D_{10}

Table 1.2: The conjugacy classes of maximal Frobenius subgroups of A_5.

primes 3 and 5 respectively). Therefore A_5 is a CA-group with three conjugacy classes of maximal Frobenius subgroups, one for each of its maximal Frobenius kernels – which by Proposition 1.2.3, we have just laid out. This information is summarized in Table 1.2. For each maximal Frobenius kernel, the Frobenius complement is listed below. It's easy to check that the elements of the complement are the only ones in A_5 that normalize the elements of the kernel.

Another example of a CA-group is $\mathrm{SL}_2(\mathbb{F}_8)$. This group has order $2^3 \cdot 3^2 \cdot 7$. A Sylow 2-subgroup P is normalized by a Sylow 7-subgroup, R. A Sylow 3-subgroup Q and a Sylow 7-subgroup R are both normalized and inverted by subgroups of order 2, which provides the list of the three conjugacy classes of Frobenius subgroups of $\mathrm{SL}_2(\mathbb{F}_8)$. Note that not only are the Frobenius complements in A_5 cyclic, but those in $\mathrm{SL}_2(\mathbb{F}_8)$ are also cyclic. The next proposition establishes a uniformity in this structure of the Frobenius complement.

Proposition 1.2.4. *If G is a Frobenius group that is also a CA-group, then a Frobenius complement is cyclic.*

Proof. The Frobenius complement E acts by conjugation on K so by Sylow's Theorem it acts by conjugation on some (abelian) Sylow p-subgroup K_p in K. We then define $\mathcal{K} = \{x \in K_p \mid x^p = 1\}$. Then $\mathcal{K}$ is isomorphic to a direct product of Z_p with itself n times, for some $n \in \mathbb{Z}^+$. Therefore $\mathcal{K}$ is an n-dimensional vector space over $\mathbb{F}_p$ on which E acts by conjugation and $|\mathcal{K}|$ is relatively prime to any p dividing $|K|$. By Theorem 1.0.2 (Schur's Lemma) applied to any (abelian) Sylow q-subgroup $A \leq E$, using the fact that $C_K(a) = 1$ for all nonidentity $a \in A$, we see that A must be cyclic. So every Sylow subgroup of E is cyclic. By [7, Theorem 7.6.2], E is solvable. Thus E has a normal subgroup R of order r for some prime

r. By [5, Theorem 25.6], it follows that $R \leq Z(E)$. Thus $E \leq C_G(R)$ is abelian and hence cyclic as claimed. ■

Having established the structure of Frobenius subgroups within a CA-group, we now present a conclusive proposition which includes a class equation for CA-groups. This class equation plays an integral role in Suzuki's proof that all odd order CA-groups are solvable, so we will see it again in the next chapter.

Proposition 1.2.5. *Let G be a minimal simple CA-group with maximal abelian subgroups $K_1, K_2, \cdots, K_n$ representing all of the distinct conjugacy classes of maximal abelian subgroups of G. By Proposition 1.2.3 their normalizers represent all distinct conjugacy classes of maximal Frobenius subgroups of G with Frobenius complement $E_1, E_2, \cdots, E_n$ respectively where $N_G(K_i) = K_iE_i$ for every $i = 1, 2, \cdots, n$. Then the following hold:*

1. *For every $i \neq j$, $gcd(|K_i|, |K_j|) = 1$.*
2. *$\prod_{i=1}^{n} |K_i| = |G|$.*
3. *Every nonidentity element of G is conjugate to an element of exactly one K_i.*
4. *$|G| = 1 + \sum_{i=1}^{n} \frac{k_i - 1}{k_i n_i}|G|$ where $|K_i| = k_i$, $|E_i| = e_i$, and $e_i > 1$ for every i such that $1 \leq i \leq n$.*
5. *Two elements x, $y \in G$ are conjugate if and only if they have conjugates x_1, y_1 respectively in the same K_i and x_1, y_1 are conjugate in $N_G(K_i)$.*

Proof. To prove part (1), we use a proof by contrapositive. Let p be a prime dividing $|K_i|$ and $|K_j|$, and $P \in \mathrm{Syl}_p(G)$. We can fix P so that $P \leq K_i$ and then there exists $g \in G$ such that $P \leq K_j^g$, since Proposition 1.2.3 established that the K_i are π-Hall subgroups. Then $K_i \cap K_j^g \neq 1$ so there exists a nonidentity x in the intersection. Since K_i is abelian, $K_i \leq C_G(x)$ but K_i is a maximal abelian subgroup. Therefore we have $C_G(x) = K_i$. Similarly, $K_j^g = C_G(x)$ and so K_i is a conjugate of K_j which means that $i = j$. Thus if $i \neq j$ there is no prime p dividing both $|K_i|$ and $|K_j|$.

For part (2), let p be a prime such that $p \bigm| |G|$ and let $P \in \mathrm{Syl}_p(G)$. The subgroup P is abelian, therefore it is a subgroup of some maximal abelian subgroup – so $P \leq K_i$ for some i. Thus p divides $\prod_{i=1}^{n} |K_i|$ to the same power that it divides $|G|$. Therefore $|G| = \prod_{i=1}^{n} |K_i|$.

Consider a nonidentity $x \in G$. Each K_i is TI so if $x \in K_i$, then x is not in any distinct conjugate of K_i. Since $|K_i|$ and $|K_j|$ are relatively prime for every $i \neq j$, if $x \in K_i \cap K_j$ then $|x| = 1$. Thus each nonidentity $x \in G$ is conjugate to an element of exactly one K_i. Thus part (3) is established.

Let $|K_i| = k_i$ and $|E_i| = e_i$ for every $i = 1, 2, \cdots, n$. Then

$$|G| = 1 + \sum_{i=1}^{n} (n_i - 1)(\text{the number of conjugates of } K_i)$$

simply by counting each element. The number of conjugates of K_i is $|G : N_G(K_i)|$ so part (4) follows easily. Note that $K_i < N_G(K_i)$ by Theorem 1.1.13 and the simplicity of G, *i.e.*, $e_i > 1$.

For the forward direction of part (5), let x and y be conjugate in G. It's clear then that there exists x_1 and y_1 elements of the same K_i where x_1 is a conjugate of x and y_1 is a conjugate of y. Then $x_1^t = y_1$ for some $t \in G$ so $y_1 \in K_i$ and $y_1 \in K_i^t$. Since K_i is a TI-set, $t \in N_G(K_i)$. Therefore x_1 and y_1 are conjugate in $N_G(K_i)$. The reverse implication is trivial since conjugation is an equivalence relation. ■

The next corollary follows immediately from part (5) of the previous proposition.

Corollary 1.2.6. *Under the same assumptions as in Proposition 1.2.5, the number of conjugacy classes in* G *is* $1 + \sum_{i=1}^{n} \frac{k_i - 1}{e_i}$.

The preceding theorems and propositions regarding CA-groups are well established in the literature. A thorough understanding of the structure of CA-groups is crucial for understanding the difficulty they have presented in proving that every odd order group is solvable. We next will be discussing the efforts of Suzuki and Burnside regarding CA-groups, in Chapter 2.

Chapter 2

Significant Efforts and Suzuki's Proof

While simple groups have been fascinating since their definition, the drive to identify all simple groups began around the close of the 19^{th} century. As mentioned, the observation by Burnside that known odd order groups were solvable began a quest to extend that observation as far as possible. This chapter begins in Section 2.1 by discussing Burnside's method of approach and how this method first encountered CA-groups as minimal counterexamples. We also give an independent proof of how a particularly "troublesome" CA-group can be shown solvable. We will be revisiting this group as an interesting example throughout the remaining discussion. Additionally, we introduce a new example of a CA-group similar to the one which is known for giving Burnside pause. In Section 2.2 we outline the proof given by Suzuki that all odd order CA-groups are solvable. We also apply the methods in the proof to the group A_5 to show how even order CA-groups escape the net Suzuki built, and to illustrate the elusive qualities within the proof.

2.1 Case-by-Case Strategy

To answer his conjecture, stated at the outset of this thesis, William Burnside adopted a case-by-case approach to showing that every nontrivial odd order group is solvable, using group-theoretic methods. He began by showing that all groups divisible by two primes are solvable. Notice that his strategy did not force the primes to be distinct, so he began with groups of order p^2 or pq for distinct odd primes p and q. Burnside then quickly moved on to groups whose order is divisible by three primes, meaning groups of order p^3, p^2q, or pqr for distinct odd primes p, q, and r. Eventually Burnside was able to show that groups whose order was divisible by up to seven odd primes were all solvable, with the exception of a group of order $3^3 \cdot 7 \cdot 13 \cdot 409$. This potential counterexample was a CA-group, and Burnside had to resort to character theory to prove, finally, that it *is* solvable. Let us explore this exceptional group to understand why Burnside had so much trouble pinning it down.

Consider a CA-group G of order $3^3 \cdot 7 \cdot 13 \cdot 409$. If we assume that such a group is simple, then it can be shown that the Sylow 3-subgroup must be normalized by a Sylow 13-subgroup, and each of the other Sylow subgroups are normalized by subgroups of order 3, using Sylow's Theorems. Thus the order of a normalizer of any Sylow subgroup is divisible by exactly two distinct primes. It can be shown that in G there are no elements of composite order or of order 9 so the Sylow normalizers turn out to be Frobenius groups whose kernels are TI-sets in G as described in Proposition 1.2.5 (with $n = 4$). We can check to see if G satisfies the class equation:

$$\begin{aligned}|G| &= 1 + (3^3 - 1)(4 \cdot 409) + (7-1)(3^2 \cdot 13 \cdot 409) + \\ &\qquad (13-1)(3^2 \cdot 7 \cdot 409) + (409-1)(3^2 \cdot 7 \cdot 13) \\ &= 3^3 \cdot 7 \cdot 13 \cdot 409.\end{aligned}$$

All in all, there is no apparent contradiction – no immediate reason why such a simple group G could not exist. In [4, Chapter 19.3], there is a beautiful character theory proof of nonexistence. Here we give an elementary permutation group theory proof, which gives the flavor of the approach we take in Chapter 3 to proving that certain CA-groups must be solvable.

Proposition 2.1.1. *A simple group of order* $3^3 \cdot 7 \cdot 13 \cdot 409$ *does not exist.*

Proof. Assuming such a group G exists, elementary calculations using only Sylow's Theorem show it must be a CA-group, and we have already discussed the Sylow subgroup structure G must have. Let $r = 409$. If $R \in \mathrm{Syl}_r(G)$ then the order of $N_R = N_G(R)$ is $409 \cdot 3$. Thus $|G : N_R| = 3^2 \cdot 7 \cdot 13$ and so G is isomorphic to a subgroup of S_{819}, meaning that G has a permutation representation of degree 819. Let $R = \langle x \rangle$ where $|x| = 409$. Then G acts by left multiplication on the left cosets of N_R such that $xgN_R = gN_R$ if and only if $g^{-1}xg \in N_R$. The order of $g^{-1}xg$ is that of x, and as $R \trianglelefteq N_R$ we know that $g^{-1}xg \in N_R$ if and only if

$$g^{-1}\langle x \rangle g = \langle x \rangle = R,$$

which occurs if and only if $g \in N_G(R) = N_R$. (Equivalently, we can consider G acting by conjugation on the 819 Sylow 409-subgroups with N_R also the stabilizer of the point R.) So x fixes only the coset N_R. It must therefore shuffle the remaining 818 elements, in cycles of size 409. Thus x has a cycle decomposition of two 409-cycles and one 1-cycle. This establishes the action of $x \in R$ on the 819 points.

Given the order of N_R, there must exist y with order three such that y normalizes $\langle x \rangle$ and $N_R = \langle x \rangle \langle y \rangle$. We will use this element y to arrive at a contradiction. The element y permutes the orbits of $\langle x \rangle$, such that $\mathcal{O}_\infty$ and $\mathcal{O}_\in$ correspond to the two orbits of size 409 and $\mathcal{O}_\ni$ corresponds to the orbit of size one. But y can potentially only switch $\mathcal{O}_\infty$ and $\mathcal{O}_\in$ because of size considerations. If y were to switch these two orbits though, it would have to have even order which contradicts the fact that y has order 3. Thus y must fix all three orbits. By Corollary 1.1.7 applied to each of $\mathcal{O}_\infty$ and $\mathcal{O}_\in$ we see that y fixes exactly one point in each orbit of $\langle x \rangle$. Therefore y fixes exactly one point in each of the three orbits and exactly three points overall. Since G has one class of subgroups of order 3 (by the action of an element of order 13 on a Sylow 3-subgroup), every element of order 3 in G has exactly 3 fixed-points in its cycle decomposition as a permutation in S_{819}.

Let P be a Sylow 3-subgroup of G and consider an element of order 13 in $N_P = N_G(P)$. This element must act by conjugation without nontrivial fixed-points on P, thus P is isomorphic to $Z_3 \times Z_3 \times Z_3$. Choose P so that $y \in P$. Let $\mathcal{R}$ be the set of fixed-points of y acting on 819 points. We know that the cardinality of $\mathcal{R}$ is three. The element y commutes with P, therefore $\langle y \rangle \trianglelefteq P$

and so P acts on $\mathcal{R}$. Thus there exists a map from P into $S_{\mathcal{R}} \cong S_3$ and so some subgroup of P of order greater than or equal to 9 fixes each point of $\mathcal{R}$. Thus some subgroup of order 9 normalizes a Sylow 409-subgroup. This contradicts the fact that $|N_R| = 409 \cdot 3$ and so completes the proof. ■

The case of the CA-group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ gives a taste of how tricky it can be to show that a particular CA-group is solvable. The order $3^3 \cdot 7 \cdot 13 \cdot 409$ is what we call a *Burnside number*, the order of a "potentially" simple CA-group of odd order.

We have discovered another Burnside number through the course of our research: $3^7 \cdot 13 \cdot 41 \cdot 547 \cdot 1093 \cdot 4493$. As in the preceding case, a simple CA-group G of this order would have four conjugacy classes of Frobenius subgroups. Sylow 3-subgroups are each normalized by a Sylow 1093-subgroup; these normalizers compose one of the conjugacy classes of maximal Frobenius subgroups. The Sylow 1093-subgroups and the Sylow 547-subgroups would then compose the next two conjugacy classes of Frobenius kernels, where each of these Sylow subgroups would be normalized by a subgroup of order 3. The remaining conjugacy class of Frobenius kernels would be represented by a cyclic subgroup of order $13 \cdot 41 \cdot 4493$. A Frobenius kernel of this class would also be normalized by a subgroup of order 3.

Such an example was developed by noting that 7 is the first exponent x after 3 for which the fraction $\frac{3^x-1}{2}$ is prime. Thus the prime 1093 plays a role analogously to that of 13 in the $|G| = 3^3 \cdot 7 \cdot 13 \cdot 409$ example. The prime $547 = (1093+1)/2$ plays a similar role to that of $7 = (13+1)/2$. Having determined representatives for these three conjugacy classes of Frobenius subgroups of a potentially simple CA-group, one can use the class equation to determine the order of a representative of the remaining conjugacy class of Frobenius kernels, assuming that the Sylow 3-subgroup is elementary abelian. Let this remaining conjugacy class of Frobenius kernels be represented by a subgroup of order r. Then the class equation is:

$$\begin{aligned}|G| &= 3^7 \cdot 547 \cdot 1093 \cdot r \\ &= 1 + (3^7-1)547r + (1093-1)3^6 \cdot 547r + (547-1)3^6 \cdot 1093r + (r-1)3^6 \cdot 547 \cdot 1093.\end{aligned}$$

The order of the group is determined once the order of three representatives of distinct conjugacy classes of Frobenius subgroups have been determined. In the case of the CA-group of order $3^3 \cdot 7 \cdot 13 \cdot 409$, the order of the group demands the remaining factor be prime – namely 409. In the case of this new CA-group, however, the order of the group does not place the same demand on the remaining Frobenius kernels and in fact $r = 13 \cdot 41 \cdot 4493$. The proof that this new example is solvable is similar to the proof of Proposition 2.1.1.

Theorem 2.1.2. *There is no simple CA-group of order* $3^7 \cdot 13 \cdot 41 \cdot 547 \cdot 1093 \cdot 4493$ *as described above.*

Proof. Assume otherwise. Let $p = 3$, $q = 547$, and $s = 1093$. Then $|G| = p^7 qrs$ and representatives of the distinct conjugacy classes of Frobenius kernels as described in Proposition 1.2.5 have order p, q, r, and s. Let P be a representative of the conjugacy class of Frobenius kernels of order p^7, and likewise for R. Given this notation, $N_G(R) = RP_0$ where P_0 is a subgroup of order 3. We can fix $P \in \mathrm{Syl}_p(G)$ so that $P_0 \leq P$. Let Ω_r be the set of conjugates of R in G, so that $|\Omega_r| = |G : N_G(R)| = 3^6 \cdot 547 \cdot 1093$ and G acts transitively on Ω_r by conjugation.

Because R is a TI-subgroup, the normalizer of R acts on Ω_r with R fixing exactly one point and cycling the remaining points in orbits of size r. The number of r-cycles is $(|\Omega_r| - 1)/r = 182$. An element of order three then fixes at most one point in each orbit of R on Ω_r by Corollary 1.1.7, hence fixes at most 183 points. Then P must be able to act on these 183 points with P_0 fixing each, but no element of $P - P_0$ can fix any of the points fixed by P_0 (since 9 does not divide $|N_G(R)|$). However, note that $|P/P_0| = 3^6 > 183$ so in fact P cannot act in this way on these fixed-points. Thus a contradiction has been found and the group cannot be simple. ∎

Considering the two exceptional cases discussed in this section, it's believable that given any CA-group of a fixed order, one might eventually find an elementary group-theoretic proof that the group is solvable. The question for this thesis is: Why can we not devise a group-theoretic proof to handle all CA-groups at once?

In 1957, Michio Suzuki proved that all odd order CA-groups are solvable but his proof, which we now outline, resorted to character theory to prove solvability.

2.2 Suzuki's Proof

Theorem 2.2.1 ((Suzuki)). *Every CA-group of odd order is solvable.*

In this section we describe Suzuki's proof of Theorem 2.2.1, above. The argument we give is more streamlined than Suzuki's in [11] and [12], using arguments of Feit and Thompson from [6]. We first develop insight into the exceptional characters of a CA-group. The proof of the theorem relies on understanding the particulars of a class function, to place a bound on the order of a minimal counterexample group. After proving Theorem 2.2.1, we exhibit the mechanics of the proof using the example of A_5, a simple CA-group of even order. In all of the propositions of this section the group is an odd-order CA-group, G, as described in Section 1.2. By the results of that section we may further assume that G is a minimal counterexample to Suzuki's Theorem, hence G is simple, non-abelian, and every proper subgroup is solvable.

Proposition 2.2.2. *Given a CA-group G, fix a maximal Frobenius subgroup N with abelian Frobenius kernel K. Let N have w irreducible characters ζ_j, each without K in the kernel. Define $\alpha_{jk} = \zeta_j - \zeta_k$. Then:*

1. *There exist fixed $\varepsilon = \pm 1$ and distinct irreducible characters χ_j of G, all of the same degree, so that $\alpha_{jk}^* = \varepsilon(\chi_j - \chi_k)$. (Recall that * indicates inducing class functions from any subgroup up to the whole group G.)*
2. *The value of ε is independent of j and k, and is uniquely determined if $w \geq 3$.*
3. *If $x \in G$ is not conjugate to a nonidentity element of K then $\alpha_{jk}^*(x) = 0$ for every $j, k \leq w$.*
4. *Let $x \in G$. If x is not conjugate to a nonidentity element of K then $\chi_j(x) = \chi_k(x)$ for every $j, k \leq w$.*

Proof. The proof of parts (1) and (2) is by inspection of each case. First note that for $j \neq k$, we have $2 = ||\alpha_{jk}||_N^2 = ||\alpha_{jk}^*||_G^2$ by Proposition 1.1.12. Thus α_{jk}^* is the difference of two distinct irreducibles of G.

If $w = 2$ then the proposition is proven by the above. In the case that $w = 3$, again by Proposition 1.1.12, $(\alpha_{12}^*, \alpha_{13}^*)_G = (\alpha_{12}, \alpha_{13})_N = 1$. Let the character common to the induced characters be χ_1. Then let the other irreducible character of α_{12}^* be χ_2. This uniquely determines χ_2 and ε. This also uniquely determines χ_3 in α_{13}^*. Since $(\alpha_{12}^*, \alpha_{13}^*)_G = 1$, the coefficient on χ_1 in both characters' decompositions is the same, ε. Thus $\alpha_{13}^* = \varepsilon(\chi_1 - \chi_3)$. It's easily checked that $\alpha_{23}^* = \varepsilon(\chi_2 - \chi_3)$.

When $w \geq 4$, similar considerations uniquely determine ε, χ_1, χ_2, and χ_3. Examine α_{1k}^* to show that χ_j is uniquely determined, for $j = 4, 5, \ldots, w$. Thus parts (1) and (2) are established.

To show part (3), recall that every ζ_j is a character induced from a nonprincipal irreducible character of K to N, so there exists a degree 1 character φ_j of K such that $\widetilde{\varphi_j} = \zeta_j$. The formula for induction yields the remainder of the result.

By (3), if an element $x \in G$ is not conjugate to some nonidentity element of K then for every j, k between 1 and w we have that $0 = \alpha_{jk}^*(x) = \varepsilon\chi_j(x) - \varepsilon\chi_k(x)$. Therefore $\chi_j(x) = \chi_k(x)$. ∎

The characters χ_j are called *exceptional characters of G with respect to K*. Critical properties of exceptional characters are summarized in Proposition 2.2.4 and Corollary 2.2.5. The proof of Proposition 2.2.4 requires an additional lemma of Burnside.

Lemma 2.2.3 ((Burnside))**.** *Let G be any odd order group and χ any nonprincipal irreducible character of G. Then $\chi \neq \overline{\chi}$, where $\overline{\chi}$ is the complex conjugate of χ.*

Proof. Assume, by way of contradiction, that $\chi = \overline{\chi}$. Recall that for an odd order group G, no nonidentity element $x \in G$ is conjugate to its inverse. We may then list the nonidentity elements of G in pairs, x, x^{-1}, and then subdivide G by letting G_0 be a subset of G containing exactly one of each pair. Then we have:

$$G = \{1\} \cup G_0 \cup G_0^{-1}.$$

Also recall that $\overline{\chi(g)} = \chi(g^{-1})$. So for every $g \in G$ we have $\chi(g) = \chi(g^{-1})$. Since χ is orthogonal to the principal character of G, 1_G, we have:

$$\begin{aligned} 0 = |G|(\chi, 1_G)_G &= \sum_{g \in G} \chi(g) \\ &= \chi(1) + \sum_{g \in G_0} \chi(g) + \sum_{g \in G_0^{-1}} \chi(g) \\ &= \chi(1) + \sum_{g \in G_0} (\chi(g) + \chi(g^{-1})) \\ &= \chi(1) + 2 \sum_{g \in G_0} \chi(g). \end{aligned}$$

Thus $\chi(1)/2 = \sum_{g \in G_0} \chi(g)$, which is an algebraic integer [4, Proposition 18.14]. Since $|G|$ is odd and $\chi(1)$ must divide $|G|$, we have that $\chi(1)/2$ is not in $\mathbb{Z}$, which is a contradiction. Therefore $\chi \neq \overline{\chi}$. ■

Proposition 2.2.4. *If χ is exceptional for some K then for every $\sigma \in$ Aut $(\overline{\mathbb{Q}})$ we have that χ^σ is also exceptional with respect to K. In particular, this means that $\overline{\chi}$ is exceptional for the same K and $\varepsilon(\chi - \overline{\chi}) = \alpha^*_{jk}$ for some $j \neq k$.*

Proof. If χ is exceptional with respect to some K then $(\chi, \alpha^*_{jk})_G \neq 0$ for some $j, k \leq w$. Considering the formula for inner products, it's easy to see then that $(\chi^\sigma, (\alpha^*_{jk})^\sigma)_G \neq 0$. Then $\alpha^{*\sigma}_{jk} = \alpha^{\sigma *}_{jk} = (\zeta^\sigma_j - \zeta^\sigma_k)$. As ζ^σ_j and ζ^σ_k are distinct irreducible characters of N induced from K, there exists $p, q \leq w$ such that $\zeta^\sigma_j - \zeta^\sigma_k = \zeta_p - \zeta_q$. So $\alpha^{*\sigma}_{jk} = \alpha^*_{pq}$, and χ^σ is also exceptional with respect to K. The last assertion of the proposition follows easily from Lemma 2.2.3. ■

Corollary 2.2.5. *The characters exceptional to K are integer-valued on elements x that are not conjugate to an element of K.*

Proof. Let χ be a character exceptional with respect to K. By Proposition 2.2.4, χ^σ is also exceptional with respect to K for every $\sigma \in$ Aut $(\overline{\mathbb{Q}})$. Given an element $x \in G$ with x not a conjugate of a nonidentity element from K, Proposition 2.2.2 part (4) implies that $\chi(x) = \chi^\sigma(x)$, for every σ. Thus $\chi(x)$ is in the fixed field of all such automorphisms and so $\chi(x)$ must be rational. For $\chi(x)$ to be rational and an algebraic integer implies that $\chi(x) \in \mathbb{Z}$. Thus the characters exceptional to K are integer valued on elements that are not conjugate to those of K. ■

Let us now introduce notation to differentiate between the exceptional characters with respect to nonconjugate Frobenius kernels. Let the CA-group G have n conjugacy classes of Frobenius subgroups, with N_i the i^{th} such subgroup. Then $N_i = K_iE_i$ where K_i is the Frobenius kernel having order k_i and a Frobenius complement E_i has order e_i. Let $\{\zeta_1^i, \zeta_2^i, \cdots, \zeta_{w_i}^i\}$ be the w_i irreducible characters of N_i without K_i in the kernel. We can then denote the exceptional characters associated with K_i by χ_j^i where $\alpha_{jk}^{i*} = \varepsilon_i(\chi_j^i - \chi_k^i)$ is the induction to G of $\alpha_{jk}^i = (\zeta_j^i - \zeta_k^i)$. If no superscript is given for an exceptional character or a character previously specified to be associated with a Frobenius subgroup, assume that character is associated with K_1. If no subscript is given for a Frobenius subgroup or its kernel, assume likewise that $i = 1$.

We can now consider exceptional characters with respect to nonconjugate Frobenius kernels, establishing a fixed relationship.

Proposition 2.2.6. *The exceptional characters with respect to K_i and K_p are distinct for every $i \neq p$.*

Proof. Let $i \neq p$ and consider the formula for the inner product of α_{jk}^{i*} with α_{qr}^{p*}.

$$(\alpha_{jk}^{i*}, \alpha_{jk}^{p*})_G = \frac{1}{|G|}\sum_{x\in G} \alpha_{jk}^{i*}(x)\overline{\alpha_{qr}^{p*}(x)}$$

Recall that $|K_i|$ and $|K_p|$ are relatively prime by Proposition 1.2.5. Then Proposition 2.2.2 part (3) asserts that since $i \neq p$, the only element on which both α_{jk}^{i*} and α_{jk}^{p*} could be nonzero would be the identity, but by definition these generalized characters are both zero on the identity. We then see that every term in the sum is zero, and the inner product is therefore zero. Let us now expand the inner product in terms of the exceptional characters of G.

$$\begin{gathered}(\alpha_{jk}^{i*}, \alpha_{jk}^{p*})_G = (\varepsilon_i(\chi_j^i - \chi_k^i), \varepsilon_p(\chi_q^p - \chi_r^p))_G = 0\\ \Rightarrow ((\chi_j^i - \chi_k^i), (\chi_q^p - \chi_r^p))_G = 0\\ \Rightarrow (\chi_j^i, \chi_q^p)_G + (\chi_k^i, \chi_r^p)_G - (\chi_j^i, \chi_r^p)_G - (\chi_k^i, \chi_q^p)_G = 0\end{gathered}$$

As the characters exceptional to the same Frobenius kernel are distinct, inspection of the terms forces them all to equal zero (note that $(\chi, \chi')_G = 0$ or 1 accordingly as $\chi \neq \chi'$ or $\chi = \chi'$ respectively, for irreducible characters χ and χ'). Thus the exceptional characters with respect to K_i are distinct from those exceptional to K_p, for $i \neq p$. ∎

Lemma 2.2.7. *Every nonprincipal irreducible character of G is exceptional with respect to some K_i for some i such that $1 \leq i \leq n$.*

Proof. The proof of this lemma relies on counting up the conjugacy classes of G from Corollary 1.2.6 and observing that total equals the number of exceptional characters from Propositions 2.2.2 and 2.2.6. ∎

Proposition 2.2.6 and Lemma ref2.9 yield a manner of working with the characters of G, through the fact that each nonprincipal irreducible character is exceptional with respect to exactly one Frobenius kernel. We know how to create exceptional characters, and exactly how many there are with respect to a particular Frobenius kernel, so the irreducible characters of G are "within our grasp," even if we do not know their degrees.

The next proposition provides the backdrop required specifically to prove Theorem 2.2.1. We begin by renumbering the representative maximal Frobenius subgroups of G so that $e_1 \leq e_2 \leq \cdots \leq e_n$. If there are two subgroups with the same size complement then the subgroup with the larger Frobenius kernel is given smaller index.

Proposition 2.2.8. *Define $\beta = (\widetilde{1_K - \zeta_1})^* = (1_K - \varphi_1)^*$ for some nonprincipal irreducible character φ_1 of $K = K_1$ with $\widetilde{\varphi_1} = \zeta_1$ (where 1_K is the principal character of K). Then:*

1. *The character β is zero on elements that are not conjugate to an element of K.*

2. *$||\beta||_G^2 = e + 1$.*

Proof. Part (1) of the proposition follows from the formula for induction. To show part (2), note that β is a class function, and $\beta(1) = e - e = 0$. By Proposition 1.1.12,

$$\begin{aligned} ||\beta||_G^2 &= ||\widetilde{1_K} - \zeta_1||_N^2 \\ &= ||\rho_{N/K} - \zeta_1||_N^2 \\ &= ||\rho_{N/K}||_N^2 + || - \zeta_1||_N^2 \\ &= e + 1, \end{aligned}$$

where the third equality holds because $\rho_{N/K}$ has K in its kernel but by definition ζ_1 does not, so these two characters are orthogonal. This proves (2). ■

The class function β will lead to a bound on the order of a simple nontrivial CA-group G. For this reason, we further explore the characteristics of β through its decomposition, in Proposition 2.2.9.

Proposition 2.2.9. *Let the definition of β be the same as in Proposition 2.2.8. If Δ is defined as $\Delta = \chi_1 + \chi_2 + \cdots + \chi_w$ (the sum of all exceptional characters associated with K_1), then the decomposition of β is given by*

$$\beta = 1_G - \varepsilon_1\chi_1 + a\Delta + \Gamma$$

where $\varepsilon_1 = \pm 1$, $a \in \mathbb{Z}$, and Γ is a real-valued generalized character whose irreducible constituents are exceptional for subgroups K_i for $i \geq 2$ and with $||\Gamma||_G^2 \leq e - 1$.

Proof. We shall proceed with the proof of Proposition 2.2.9 in steps. The first step is to show that the principal character of G is a constituent of β of multiplicity 1. Consider the inner product of β with 1_G, which reduces as follows by Frobenius reciprocity:

$$\begin{aligned} (\beta, 1_G)_G &= (1_K - \varphi, 1_{G|K})_K \qquad \text{where } \varphi \text{ induces to } \zeta_1 \text{ in } K \\ &= (1_K - \varphi, 1_K) \\ &= 1. \end{aligned}$$

Thus β contains exactly 1 copy of 1_G.

The next step is to show that, except for χ_1, the characters exceptional with respect to K appear with the same multiplicity. Consider $(\beta, \chi_j)_G$. By Proposition 1.1.12, we have that

$$(\beta, \alpha_{1k}^*)_G = (\widetilde{1_k} - \zeta_1, \zeta_1 - \zeta_k)_N = -1$$

for every $k > 1$. Then because $\alpha_{1k}^* = \varepsilon(\chi_1 - \chi_k)$, we have that $(\beta, \chi_1 - \chi_k)_G = -\varepsilon$ for every $k > 1$. But then we also have

$$(\beta, \chi_1 - \chi_k)_G = (\beta, \chi_1)_G - (\beta, \chi_k)_G.$$

Thus $(\beta, \chi_1)_G + \varepsilon = (\beta, \chi_k)_G$. Let $c = (\beta, \chi_1)_G$ and $a = c + \varepsilon$. Then $(\beta, \chi_k)_G = a$ for every $k > 1$. Thus

$$\beta = 1_G + a(\chi_2 + \cdots + \chi_w) + c\chi_1 + \text{ characters orthogonal to } 1_G, \chi_1, \cdots, \chi_w.$$

We can further simplify β by allowing the orthogonal characters at the end to be called Γ, and recognizing that $a - c = \varepsilon$. Therefore we can write β as:

$$\beta = 1_G + a\Delta - \varepsilon\chi_1 + \Gamma$$

where Γ is composed of characters exceptional with respect to K_i for $i \geq 2$.

We finally come to consideration of Γ. There are two items to note:

First, $||\beta||^2 = e + 1$, and even if $a = 0$, ε is equal to ± 1 so there is at least one copy of χ_1 in the decomposition of β and one copy of the principal character. Therefore, $||\Gamma||^2$ is less than or equal to $(e + 1) - 2 = e - 1$.

Second, recall that $(\beta, \alpha_{jk}^{i*})_G = 0$ for every $i \geq 2$. In particular, $(\beta, \varepsilon_i(\chi_j^i - \overline{\chi_j^i})) = 0$ so the number of copies of χ_k^i in β is equal to the number of copies of its complex conjugate. This means that for all $i \geq 2$ and all j, both χ_j^i and its complex conjugate are components of Γ with the same multiplicity (possibly zero). Therefore, Γ is real valued.

Now we need to show that Γ is integer-valued on elements of G. Consider the algebraic conjugates of a constituent of Γ. If χ_j^i is a component of Γ and $\chi_j^{i\sigma}$ is one of its algebraic conjugates then we have two possibilities:

1. $\chi_j^i = \chi_j^{i\sigma}$ so both occur in Γ with equal multiplicity; or

2. $\chi_j^i \neq \chi_j^{i\sigma}$, in which case the above argument with complex conjugates would work to show that they must both occur in Γ with equal multiplicity.

Therefore, in either case, $\Gamma(x)$ is a sum of algebraic integers for every $x \in G$, and the sum of all algebraic conjugates of $\chi_j^i(x)$ for any $\chi_j^i \in \Gamma$. Thus Γ is integer valued on every element of G. ■

Armed with the preceding lemmas and propositions, we are now ready to give a proof of Theorem 2.2.1, as stated at the beginning of the section.

Proof. Let us divide the indexing set of Frobenius kernels into two subsets:

$$\mathcal{A} = \{i \geq 2 \mid \chi^i \perp \beta \text{ for every exceptional character } \chi^i \text{ associated to } K_i\};$$

$$\mathcal{B} = \{i \geq 2 \mid \text{there exists } j \text{ with exceptional character } \chi_j^i \text{ and } (\chi_j^i, \beta)_G \neq 0\}.$$

These sets $\mathcal{A}$ and $\mathcal{B}$ are clearly disjoint with $\{1\} \cup \mathcal{A} \cup \mathcal{B} = \{1, 2, \cdots, n\}$. We shall proceed from here in three steps. The first step will be to gain an upper bound on $\Sigma_{i \in \mathcal{B}} \frac{k_i - 1}{k_i e_i}$, and the second to find an upper bound on the similar summation associated with $\mathcal{A}$. This will allow us to, in step three, place a bound on $|G|$.

Step 1. $\sum_{i \in \mathcal{B}} \frac{k_i - 1}{k_i e_i} \leq \frac{e-1}{2e_2}$.

If $i \in \mathcal{B}$ then for some j, the inner product $(\beta, \chi_j^i)_G$ is nonzero. Hence, Γ contains χ_j^i as a constituent; and given that $|G|$ is odd, Γ also contains an equal number of copies of $\overline{\chi_j^i}$ which by Lemma 2.2.3 is distinct from χ_j^i. Since $||\Gamma||^2$ is less than or equal to $e - 1$, we have then that $|\mathcal{B}| \leq \frac{e-1}{2}$. We also have an inequality:

$$\frac{k_i - 1}{k_i e_i} \leq \frac{1}{e_i} \leq \frac{1}{e_2},$$

given by the ordering we chose on the Frobenius kernels. We therefore have

$$\sum_{i \in \mathcal{B}} \frac{k_i - 1}{k_i e_i} \leq \frac{e - 1}{2e_2}.$$

Step 2. $\sum_{i \in \mathcal{A}} \frac{k_i - 1}{k_i e_i} \leq \frac{1}{w}$.

Let $i \in \mathcal{A}$ and $x \in K_i$. By construction of $\mathcal{A}$ and by Corollary 2.2.5, $\chi(x) \in \mathbb{Z}$ for every exceptional χ appearing in β. Since χ and $\overline{\chi}$ both appear in Δ or both appear in Γ and are distinct by Lemma 2.2.3, we have that $\Delta(x)$ and $\Gamma(x)$ are even integers. Thus $\beta(x) = 1 - \varepsilon_1\chi_1(x)$ (modulo 2), so $\chi_1(x) \neq 0$. Since $\chi_1(x) \in \mathbb{Z}$, it must be that $|\chi_1(x)| \geq 1$. Since $\chi_1(x) - \chi_j(x)$ is zero for every nonidentity $x \in K_i$, the two characters are equal on such x. Thus for every $j = 1, 2, \cdots, w$ we have that $|\chi_j(x)| \geq 1$ and therefore $|\Delta(x)| = w|\chi_1(x)| \geq w$.

Let $G_0 = \{x \mid x$ is conjugate to some nonidentity element of K_i for some $i \in \mathcal{A}\}$. Then

$$|G_0| = |G| \sum_{i \in \mathcal{A}} \frac{k_i - 1}{k_i e_i}.$$

If we view $||\Delta||^2$ as $\frac{1}{|G|}\sum_{x \in G} |\Delta(x)|^2$, then

$$\begin{aligned} w = ||\Delta||^2 &\geq \frac{1}{|G|} \sum_{x \in G_0} |\Delta(x)|^2 \\ &\geq \frac{1}{|G|}|G_0|w^2 = w^2 \sum_{i \in \mathcal{A}} \frac{k_i - 1}{k_i e_i} \end{aligned}$$

and Step 2 is complete.

Step 3. Consider for of the class equation for G in Proposition 1.2.5:

$$|G| = 1 + \sum_{i=1}^{n} \frac{k_i - 1}{k_i e_i}|G|.$$

Divide both sides by $|G|$ and then the bounds created in steps 1 and 2 can be implemented in this formula to show:

$$1 \leq \frac{1}{|G|} + \frac{k_1 - 1}{k_i e_i} + \frac{1}{w} + \frac{e - 1}{2e_2}.$$

If $w > 2$, then w must be at least 4 because $w = \frac{n_1 - 1}{e_1}$ is even. Since $e_2 \geq e_1 \geq 3$, we have

$$\begin{aligned} 1 &\leq \frac{1}{|G|} + \frac{1}{e_1} + \frac{1}{4} + \frac{1}{2} - \frac{1}{2e_1} \\ &\leq \frac{1}{|G|} + \frac{1}{2e_1} + \frac{3}{4} \\ &\leq \frac{1}{|G|} + \frac{11}{12} \end{aligned}$$

i	N_i	$\lvert K_i\rvert = k_i$	$\lvert E_i\rvert = e_i$	$w_i = \frac{k_i-1}{e_i}$
1	D_{10}	5	2	2
2	S_3	3	2	1
3	A_4	4	3	1

Table 2.1: The orders of Frobenius subgroups of A_5.

Thus $|G| \leq 12$. The groups of order less than 12 have long been determined, and there are no nonsolvable groups of order less than 12.

Therefore $w = 2$. By the ordering on the representatives of the conjugacy classes of Frobenius subgroups, $e_2 \geq e + 2$, so e_2 is at least five, as the e_i are odd. We can similarly substitute this information into the class equation for G, and see that ultimately, if $e \geq 5$ we arrive at a contradiction and if $e = 3$ then we have that the order of G is less than or equal to 70. Again, the groups of order less than 70 have long been determined, with no nonsolvable odd order groups falling into this list. ■

Using the definition in Proposition 2.2.8 and some of the results in this section, we can recreate β in the even order simple CA-group $G = A_5$. Consideration of this example clarifies how the sets $\mathcal{A}$ and $\mathcal{B}$ are formed. Despite the fact that A_5 is of even order, many of the propositions of this section still hold. Those that do not hold are dependant on Lemma 2.2.3, which requires an odd order group. The construction of β remains the same, however we cannot assume that complex conjugate characters are distinct. We begin by recalling from Section 1.2 that A_5 has three conjugacy classes of Frobenius subgroups, with pertinent information summarized in Table 2.1. From the ordering on the maximal Frobenius subgroups we can see that $N_1 \cong D_{10}$, $N_2 \cong S_3$, and $N_3 \cong A_4$. Recall the character table of D_{10} given in Section 1.1. In this table it was shown that D_{10} has three nonprincipal characters which we originally called χ_1, χ_2 and χ_3 where the first has degree 1 and the latter two have degree 2. In the terminology presented in the proof of Theorem 2.2.1, χ_2 and χ_3 should be renamed ζ_1 and ζ_2, though it does not matter which character is given which index. Remember, also, that for $i = 1$ the sub- or superscript is dropped for convenience of notation.

classes	1	(1 2 3)	(1 2)(3 4)	(1 2 3 4 5)	(1 2 3 5 4)
size	1	20	15	12	12
1	1	1	1	1	1
χ_1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_3	4	1	0	-1	-1
χ_4	5	-1	1	0	0
β	0	0	0	$\frac{5-\sqrt{5}}{2}$	$\frac{5+\sqrt{5}}{2}$

Table 2.2: Character table of A_5 and values for the class function β.

By definition, in the group A_5 the character $\beta = (\rho_{N/K} - \zeta_1)^*$. We can then directly calculate the value of β on each of the conjugacy classes of A_5 from the definition of induction. Let us summarize the character table of A_5 and give the values of β, in Table 2.2.

From the proof of Theorem 2.2.1 we know that β contains one copy of the principal character, though that can easily be checked using the inner product $(\beta, 1_G)_G$. Liberal use of the inner product reveals the exact decomposition of β as follows:

$$\beta = 1_G - \chi_3 + \chi_2,$$

which can now be checked by direct inspection. We know that G has two irreducible characters that are exceptional with respect to $N \cong D_{10}$, and that those characters are algebraic conjugates. It's easy to conclude then that those characters are χ_1 and χ_2. From the decomposition of β it is not immediately clear whether $\varepsilon = 1$ and $a = 0$ or if $\varepsilon = -1$ and $a = 1$. In either case, the question remains: The character χ_3 is exceptional to which of N_2 and N_3? Both $N_2 \cong S_3$ and $N_3 \cong A_4$ have exactly one nonprincipal irreducible character so we cannot form α^*_{jk} for either of these Frobenius subgroups. However, we can still define $\beta_2 = (\rho_{N_2/K_2} - \zeta_1^2)^*$ and similarly β_3. We know χ_1 and χ_2 are exception with respect to K_1 so then if these characters appear in the decomposition of β_2 or β_3 they must appear as part of Γ_2 or Γ_3 respectively. This allows us to redefine "exceptional" with respect to this particular situation to mean "not from the same Frobenius kernel as a constituent of Γ." The decomposition of β_2 and that of β_3

then allow us to determine that χ_3 is "exceptional" with respect to $N_2 \cong S_3$ and χ_4 is "exceptional" with respect to $N_3 \cong A_4$. Thus $\mathcal{A} = \{2\}$ and $\mathcal{B} = \{3\}$ for the group A_5.

While the proof of Theorem 2.2.1 is brilliant, it is not at all clear how the sets $\mathcal{A}$ and $\mathcal{B}$ could be characterized by using only the group theory behind an arbitrary CA-group. It is this question that emerges from Suzuki's proof that we hope to clarify in this thesis, perhaps thereby simplifying the proof that all CA-groups are solvable.

Chapter 3

New Approaches to the CA-Proof

In this chapter we present our original work. We proceeded by demonstrating that simple CA-groups must have at least three conjugacy classes of maximal Frobenius subgroups (see Proposition 1.2.5) and then closely examine the structure of particular CA-groups with order $p^a qr$ where p, q, and r are distinct primes. Our first attempt involves use of permutation-group-theoretic methods, as discussed in Section 3.2. Section 3.3 describes the use of graph theory to disprove existence of specific odd order CA-groups.

3.1 Initial Reductions

Given the information from Chapter 1, it is not difficult to arrive at further characterizations of CA-groups that prove useful in showing that all nontrivial odd-order CA-groups are solvable. Consider the following proposition.

Proposition 3.1.1. *If G is a solvable CA-group then G is a Frobenius group.*

Proof. Let G be a solvable CA-group. First note that G has nontrivial abelian normal subgroups: Recall that since G is solvable, G has a finite derived series with its last term, H, abelian. Let P be the unique Sylow p-subgroup of H for some prime $p \bigm| |H|$. Then P char H and $H \trianglelefteq G$, therefore $P \trianglelefteq G$. Thus P is an abelian normal subgroup of G.

Now let us show that G is a Frobenius group. Let K be a maximal abelian subgroup of G such that $K \trianglelefteq G$. The subgroup K is abelian and therefore $K \leq$

$C_G(K)$. However, G is CA so therefore $C_G(K)$ is abelian and normal in G. Since K is maximal, $C_G(K) \leq K$ and thus $K = C_G(K)$. Recall that $C_G(K) \leq C_G(x)$ for every nonidentity $x \in K$. Therefore $K \leq C_G(x)$. Again, since G is CA, we know that $C_G(x)$ is abelian and so $K = C_G(x)$. Thus G is a Frobenius group with abelian Frobenius kernel K. ∎

The effect of Proposition 3.1.1 is that a solvable CA-group has exactly one Frobenius subgroup – itself. This leads one to ask: Considering the structure of minimal simple CA-groups as described in Proposition 1.2.5, can we show that a CA-group with n conjugacy classes of maximal Frobenius subgroups actually has only one such class, indeed only one such subgroup? In the case of $n = 2$, that is exactly what can be done. The ideas in the proof of Philip Hall's Theorem can be applied to prove a special case of Burnside's $p^a q^b$ Theorem when all Sylow subgroups are abelian. These ideas, once developed in the proof of the following theorem, will allow proof that a CA-group with exactly two conjugacy classes of maximal Frobenius subgroups does not exist. The advantage of this proof is that it does not rely on character theory, as did Burnside's original proof, so this proof may indicate a new approach to studying CA-groups too.

Theorem 3.1.2 ((Burnside)). *Given a group of order $p^a q^b$ for p and q distinct primes and where every Sylow subgroup of the group is abelian, then the group is solvable.*

Proof. Let G be a minimal counterexample: a simple group of order $p^a q^b$ with abelian Sylow subgroups P and Q such that $|P| = p^a$ and $|Q| = q^b$. Without loss of generality, let $|P| > |Q|$. Consider P^x, a Sylow p-subgroup conjugate to P. We know

$$|PP^x| = \frac{|P||P^x|}{|P \cap P^x|} \leq |G|$$

and that $|P||P^x| > |G|$. Therefore $|P \cap P^x| > 1$. Let $H = P \cap P^x$ and $N = N_G(H)$. As H is a subgroup of P, which is abelian, we know that $P \leq N$; and $q \mid |N|$ since $P^x \leq N$ and $P \neq P^x$. We have that $|N| = p^a q^\beta$ where $0 < \beta < b$ (since $N_G(H) = N \neq G$). Let $Q_0 \in \mathrm{Syl}_q(N)$ and let $Q_0 \leq Q \in \mathrm{Syl}_q(G)$, so that

$Q \cap N = Q_0$ has order q^β. Using the formula for $|NQ|$ we see

$$|NQ| = \frac{|N||Q|}{|N \cap Q|} = \frac{(p^a q^\beta)q^b}{q^\beta} = p^a q^b = |G|$$

and so $NQ = G$. Thus every $g \in G$ can be written uniquely as $g = nq$ where $n \in N$ and $q \in Q$. This implies that $N^g = N^{nq} = N^q$ and we may construct a normal subgroup of G as:

$$\bigcap_{q \in Q} N^q = \bigcap_{g \in G} N^g \trianglelefteq G$$

This intersection is nontrivial because Q is abelian, therefore $Q_0 \trianglelefteq Q$ and we also have $Q_0 = Q_0^q \leq N^q$ for every $q \in Q$. This implies that $Q_0 \leq \bigcap_{q \in Q} N^q \trianglelefteq G$. Also note $|\bigcap_{q \in Q} N^q| \leq |N|$, so the intersection is proper in G. We have thus produced a nontrivial normal subgroup of G, which contradicts the fact that G is simple. ■

We can now mimic this proof to show that when a CA-group has exactly two conjugacy classes of maximal Frobenius subgroups it must be solvable. Then by Proposition 3.1.1, G is a Frobenius group. This is a contradiction (a Frobenius group has only one such class), hence we prove:

Proposition 3.1.3. *There are no CA-groups (of odd or even order) with exactly 2 conjugacy classes of maximal Frobenius subgroups.*

Proof. Let G be a CA-group with exactly two conjugacy classes of maximal Frobenius subgroups. Suppose there exists H a solvable normal subgroup of G. Then there exists $A \trianglelefteq G$ such that A is an abelian q-group, as before, and $\overline{G} = G/A$ is a CA-group by Proposition 1.2.2 (6) with at most two conjugacy classes of maximal Frobenius subgroups; hence by induction $\overline{G}$ is solvable, so G is also solvable. Therefore, by Proposition 3.1.1, G is a Frobenius group which contradicts the assumption that G has two distinct conjugacy classes of maximal Frobenius subgroups. Thus a minimal counterexample for this proposition is a simple CA-group with two conjugacy classes of maximal Frobenius subgroups.

Let G be such a minimal counterexample, with nonconjugate maximal Frobenius kernels K_1 and K_2. Let the normalizer of K_1 be denoted as N; we know from the structure of Frobenius groups that N is a representative for one of the conjugacy classes of maximal Frobenius subgroups. Let a Frobenius complement to K_1 be E. This subgroup E is abelian and so is contained in a conjugate of K_2 by Propositions 1.2.4 and 1.2.5. Let us fix K_2 so that $E \leq K_2$. This implies that $N \cap K_2 = E$ and using the formula for the order of NK_2, as we did for $|NQ|$ in the previous proof and Proposition 1.2.5(2), one can easily see that $NK_2 = G$. Thus every element $g \in G$ can be written uniquely as a product $g = nk$ where $n \in N$ and $k \in K_2$. Then $N^g = N^{nk} = N^k$ so a normal subgroup of G can be constructed:

$$\bigcap_{k \in K_2} N^k = \bigcap_{g \in G} N^g \trianglelefteq G$$

This intersection is nontrivial, as $E \trianglelefteq K_2$, an abelian group, and thus $E = E^k \leq N^k$ for every $k \in K_2$. This implies that E is contained in the intersection. As we saw in the structure of Frobenius groups as established in Proposition 1.2.5(4), E is nontrivial. Also, the intersection is contained in N, which is strictly contained in G by assumption and is solvable. Therefore we have produced a solvable normal subgroup of G. Thus G is solvable and by Proposition 3.1, G has only one conjugacy class of Frobenius subgroups, a contradiction. ■

To recap, a solvable CA-group is a Frobenius group, meaning that it has exactly one maximal Frobenius subgroup, *i.e.*, itself. Also, the ideas of the proof of Philip Hall's Theorem can be used to show that a CA-group with two conjugacy classes of maximal Frobenius subgroups must be solvable and thus there are no CA-groups with two conjugacy classes of maximal Frobenius subgroups. In the next section we consider CA-groups with at least three conjugacy classes of maximal Frobenius subgroups.

3.2 Approaches Using Permutation Group Theory

In this section we provide a group-theoretic proof of the nonexistence of simple CA-groups of order $p^a qr$ where p, q, and r are distinct odd primes, the Sylow

p-subgroup is elementary abelian, and where G has three conjugacy classes of Frobenius subgroups. We have divided this section into two parts: first, a few introductory results due to Burnside; then the bulk of the section is devoted to using these theorems on a simple CA-group following the previously stated structure.

3.2.1 Permutation Group Theory Background

In this subsection we introduce a few theorems of Burnside and derive results that are relevant to our work. In the next subsection we give these results context in the case of a simple CA-group of order $p^a qr$ for odd primes p, q, and r with a restricted subgroup structure. Let us begin with the following theorem by Burnside, with proof in [7, Theorem 7.4.3]. This theorem leads to a valuable corollary which provides restrictions on the exponent of the smallest prime dividing $|G|$ when G is a simple group.

Theorem 3.2.1 ((Burnside's N/C-Theorem))**.** *Let P be a Sylow p-subgroup of G for some prime p. If $N_G(P) = C_G(P)$, then G has a normal p-complement.*

Corollary 3.2.2. *If p is the smallest prime dividing $|G|$ and a Sylow p-subgroup of G is cyclic, then G has a normal p-complement.*

(of the corollary). Let p be the smallest prime dividing $|G|$ with the Sylow p-subgroup, P, cyclic of order p^α. The Sylow p-subgroup is cyclic so $P \leq C_G(P)$. Let $d = |N_G(P)/C_G(P)|$ and note that the factors of p in the normalizer's order are canceled out by those of the centralizer. Therefore d is a product of primes dividing $|G|$ where each is larger than p, so $\gcd(d, p) = 1$. It is also true that $N_G(P)/C_G(P) \cong M$ where $M \leq \mathrm{Aut}(P)$ and that the order of $\mathrm{Aut}(P)$ is $p^{\alpha-1}(p-1)$. Thus we have that $d \bigm| (p-1)$ yet all primes dividing d are greater than p. Accordingly it must be that $d = 1$, *i.e.*, $N_G(P) = C_G(P)$, and so we may apply Theorem 3.2.1 to conclude that G contains a normal p-complement. ■

Corollary 3.2.2 implies that if a non-abelian group is simple, then the smallest prime dividing the order of the group cannot be associated to a cyclic Sylow subgroup. In the case of a simple CA-group, we will see in the next subsection that this places restrictions on $|G|$.

The next theorem of Burnside is proven in [8, Theorem I.21.3] using character theory. The proposition following the theorem allows a close approximation without character theory that will suffice for our situation.

Theorem 3.2.3 ((Burnside))**.** *Let G be a transitive permutation group of prime degree. If G is not solvable, then it is doubly transitive.*

Proposition 3.2.4. *Let a group G act transitively on a set Ω with $|\Omega| \geq 2$. Then for any $\alpha \in \Omega$ there is a bijection between the set of orbits of G_α on Ω and the set of orbits of G acting on $\Omega \times \Omega$ (componentwise). Moreover, the order of an orbit of G on $\Omega \times \Omega$ is equal to $|\Omega| \cdot |\mathcal{O}|$ where $\mathcal{O}_\alpha$ is some orbit of G_α acting on Ω.*

(of the proposition). Let a group G act transitively on a set Ω with $|\Omega| \geq 2$. Fix $\alpha \in \Omega$. Let $\mathcal{O}$ be an orbit in the action of G on $\Omega \times \Omega$. Define $\mathcal{O}_\alpha$ as follows:

$$\mathcal{O}_\alpha = \{\beta \in \Omega \mid (\alpha, \beta) \in \mathcal{O}\}.$$

We define a bijection from the set of orbits of G acting on $\Omega \times \Omega$ to the set of orbits of G_α acting on Ω by sending an orbit $\mathcal{O} \subseteq \Omega \times \Omega$ to $\mathcal{O}_\alpha$. First note that this function is well-defined since for every $\mathcal{O}$, the set $\mathcal{O}_\alpha$ is an orbit of G_α acting on Ω. Also, since the orbits of a group action partition the set upon which the group is acting, two orbits $\mathcal{O}$ and $\mathcal{O}'$ in $\Omega \times \Omega$ are equal if and only if the corresponding $\mathcal{O}_\alpha$ and $\mathcal{O}'_\alpha$ are equal.

Now, given an orbit $\mathcal{P} \subseteq \Omega$ under the action of G_α on Ω, note that $\{\alpha\} \times \mathcal{P}$ is contained in some orbit $\mathcal{O} \subseteq \Omega \times \Omega$ since $G_\alpha \leq G$ will act transitively on this extension of $\mathcal{P}$. Then $\mathcal{P} = \mathcal{O}_\alpha$. Thus we have a bijection between orbits of G acting on $\Omega \times \Omega$ and those of G_α acting on Ω. Moreover, since we fixed $\alpha \in \Omega$, the order of the orbit $\mathcal{O}$ is $|\Omega||\mathcal{O}_\alpha|$. ■

Immediately from Proposition 3.2.4, we have the following useful corollary.

Corollary 3.2.5. *A stabilizer of a point G_α acts transitively (with one orbit) on $\Omega - \{\alpha\}$ if and only if G has one orbit on $\Omega \times \Omega$ other than the diagonal.*

A group satisfying either of the conditions in Corollary 3.2.5 is said to be *doubly transitive* in its action on Ω. Note than any doubly transitive group must have even order because $|G : G_{\alpha\beta}| = n(n-1)$ where $n = |\Omega|$ and α, β are distinct points in Ω.

We would also like to introduce a result that provides a connection between character theory and permutation theory. The following proposition is often called Burnside's Lemma (though its origins are with Frobenius) and appears in the exercises of [4, Chapter 18.3].

Proposition 3.2.6 ((Burnside's Lemma))**.** *Let G be a subgroup of S_n and for each $g \in G$ let $\pi(g)$ be the number of fixed-points of g acting on $\{1, 2, \ldots, n\}$. Let t be the number of orbits in the action of G on $\{1, 2, \cdots, n\}$. Then*

$$t|G| = \sum_{g \in G} \pi(g).$$

Proof. By definition π is the character associated with a permutation representation of G acting on $\Omega = \{1, 2, \ldots, n\}$. If we think of π as a character of G with representation $\varphi : G \to \mathrm{GL}(V)$, then the subspace $W = \{v \in V \mid \varphi(g)(v) = v \text{ for all } g \in G\}$ of V has dimension equal to $(1_G, \pi)_G$. However, the dimension of W is also the number of orbits of G acting on Ω, t. Thus

$$t = (1_G, \pi)_G = \frac{1}{|G|} \sum_{g \in G} \pi(g)$$

and the result immediately follows. (Additional details can be found in [4, Exercises 18.3.6-9].) ∎

This proposition is often proved using methods of combinatorics [1, Theorem 1.2.5], although the proof given here sketches the highlights of an elegant, classic proof. The main point in introducing Proposition 3.2.6 is to expose some of the permutation group theory hidden behind the language of character theory when a group G is acting on a set Ω. In particular, if the G is acting transitively on Ω, then $t = 1$ and so the next corollary follows.

Corollary 3.2.7. *Let G be a group acting transitively on a set Ω. Then*

$$|G| = \sum_{g \in G} \pi(g).$$

So by Corollary 3.2.7, if a group G with subgroup H is acting on the set of left cosets of H by left multiplication, then the permutation representation of this action has a character π which contains exactly one copy of the principal character of G. We will make use of this connection between the permutation representation of a group acting on left cosets of a subgroup in the next section when we show that a particular simple CA-group does not exist. Through the course of the proof, we will be examining the group as a permutation group and while we make many efforts to minimize our use of character theory, Proposition 3.2.6 and its corollary demonstrate that if the group is acting transitively on a set Ω then the inner product of the permutation representation with the principal character of the group can be thought of as a convenient means of summing the fixed-points of the group elements in the action on Ω.

3.2.2 Nonexistence of a Particular Odd Order Simple CA-Group

We may now begin to investigate the structure and characteristics of a minimal simple CA-group G with exactly three conjugacy classes of maximal Frobenius subgroups and three distinct primes dividing $|G|$. Proposition 1.20 then forces each Frobenius kernel to be not just a π-Hall subgroup but a Sylow subgroup, and incidentally allows for convenient notation for the remainder of the chapter. Let G be a simple CA-group such that $|G| = p^a qr$ where p, q, and r are distinct odd primes and assume further that the Sylow p-subgroups are elementary abelian unless otherwise specified. Let representatives of the three conjugacy classes of maximal Frobenius kernels of G be denoted as P, Q, and R, with the naturally corresponding orders: $|P| = p^a$, $|Q| = q$, and $|R| = r$. Denote the maximal Frobenius subgroup with Frobenius kernel P as $N_P = N_G(P)$, and such notation is extended to the other maximal Frobenius subgroups. Note that by Proposition 1.2.5 or Burnside's N/C-Theorem $P \neq N_P$ (and likewise for Q and

R). Recall from Chapter 1 that the Frobenius kernels of a CA-group are TI-sets; thus in this particular G the Sylow subgroups are all TI-sets. Our first proposition determines the possible order of any element in G.

Proposition 3.2.8. *Under the hypotheses of this subsection, the elements of* G *have prime order.*

Proof. For any nonidentity element $x \in G$ the element x must belong to exactly one conjugate of the maximal abelian subgroups (*i.e.*, the maximal Frobenius kernels) of G by Proposition 1.2.5 (3). Thus the order of $x \in G$ must divide the order of a Sylow subgroup. This shows the proposition for elements of the Sylow q- and r-subgroups. By assumption, the Sylow p-subgroups are elementary abelian, therefore the nonidentity elements of any Sylow p-subgroup have order p. Hence any element $x \in G$ must have prime order. ∎

Thus G has elements of order p, q, and r. Now we establish a very precise structure for the Frobenius subgroups of G.

Proposition 3.2.9. *Let* G *be a simple odd order CA-group following the hypotheses of the subsection and assume that* P *is elementary abelian. Choose notation so that* P *is normalized by a conjugate of* Q *(which is permissible since* $N_P \neq P$*). Then the following hold:*

1. *The exponent,* a*, of* p *is at least* 3.

2. $N_P = PQ$, $|N_Q| = pq$, *and* $|N_R| = pr$.

3. *The primes are ordered with* $p < q < r$.

Proof. By Corollary 3.2.2, it's clear that the smallest prime dividing $|G|$ cannot have a cyclic Sylow subgroup. This immediately implies that $p < q$, $p < r$, and that $a \geq 2$.

If $a = 2$, then either $P \cong Z_{p^2}$ or $P \cong Z_p \times Z_p$. Corollary 3.2.2 again prevents the former situation; in the latter P is abelian and therefore a subgroup of it's centralizer. Let $d = |N_P/C_G(P)|$. Then $\gcd(d, p) = 1$ as in the proof of Corollary 3.2.2. However, $|\mathrm{Aut}(P)| = |\mathrm{Aut}(Z_p \times Z_p)| = p(p+1)(p-1)$. Because p is odd, the fact that $d \;\Big|\; |\mathrm{Aut}(P)|$ forces $d = 1$. Theorem 3.2.1 then states that G has a normal p-complement contrary to G being simple. Therefore $a \geq 3$.

To prove (2), first fix Q so that P is normalized by Q. Assume that Q is not normalized by a nontrivial p-subgroup of G. Then there exists a Sylow r-subgroup R such that $N_Q = QR$. Consider the order of the subset $N_P N_Q$.

$$|N_P N_Q| = \frac{|N_P||N_Q|}{|N_P \cap N_Q|} = \frac{(p^a q)(qr)}{|N_P \cap N_Q|}$$

Since Q was fixed to be a Sylow q-subgroup that normalized P we then know that $N_P \cap N_Q = Q$. Thus $G = N_P N_Q$. By paralleling the argument of Theorem 3.1.2, we can see $Q \leq N_P$ and $Q \trianglelefteq N_Q$ so

$$Q \leq \bigcap_{n \in N_Q} N_P^n = \bigcap_{g \in G} N_P^g \trianglelefteq G.$$

Thus G has a nontrivial proper normal subgroup, a contradiction. It must therefore be the case in the minimal counterexample that Q is normalized by a nontrivial p-subgroup of G. Since the Sylow p-subgroups are elementary abelian and Frobenius complements are cyclic in a CA-group (Proposition 1.2.4), it must be that Q is normalized by a subgroup of order p.

To complete (2) assume by way of contradiction that some Sylow r-subgroup R is normalized by Q. Using Sylow's Theorems one can conclude that the number of conjugates of P is $n_p = r \equiv 1 \pmod{p}$. In fact, since P is a TI-subgroup, by [4, Exercise 6.2.21] we have that $n_p = r \equiv 1 \pmod{p^a}$. This implies that $r > p^a$. Contrariwise, $n_r = p^a \equiv 1 \pmod{r}$ which implies that $p^a > r$. Thus it must be the case that R is normalized by a nontrivial p-subgroup of G, and again, since the Sylow p-subgroups are elementary abelian, N_R has order rp.

Lastly we need to show that under this configuration $p < q < r$. As Q normalizes P, it permutes the elements of P so $q < p^a$. We also know that $|N_P| = p^a q$ so, as in the previous argument, $n_p = r \equiv 1 \pmod{p^a}$. Therefore $r > p^a$ and we have $q < p^a < r$. We already saw that p is the smallest prime, so we have the inequality

$$p < q < p^a < r$$

and are finished. ∎

Consider Proposition 3.2.9 in regards to the CA-group A_5, with order $2^2 \cdot 3 \cdot 5$. As shown in Chapter 2, A_5 has three conjugacy classes of maximal Frobenius subgroups isomorphic to A_4, S_3, and D_{10} with Frobenius kernels P, Q, and R respectively where P is the Sylow 2-subgroup, Q the Sylow 3-subgroup, and R the Sylow 5-subgroup. In this group we see that both R and Q are normalized by subgroups of order 2 and that $2 < 3 < 2^2 < 5$, as dictated by Proposition 3.2.9. The exception to part (1) of the proposition is because the prime p is even in the case of A_5.

Having exhibited the structure of a simple G following the hypotheses of this subsection, we now give proof (independent of Burnside's result on groups of prime degree) that G is of even order – a contradiction. Therefore such a G does not exist.

Proposition 3.2.10. *Let G be a simple CA-group under the hypotheses of this subsection. Then G does not exist.*

Proof. Assume G is a minimal counterexample. Though we are assuming that G has three conjugacy classes of maximal Frobenius subgroups, note that the work in Section 3.1 determined that a simple G must have at least three. Propositions 3.2.8 and 3.2.9 carefully laid out the Sylow substructure of G. This allows for determination of the "Class Equation" for G, as follows:

$$|G| = p^a qr = 1 + (p^a - 1)r + (q - 1)p^{a-1}r + (r - 1)p^{a-1}q.$$

The group G acts transitively by left multiplication (or by conjugation) on the left cosets of any subgroup $H \leq G$ (or conjugates of H respectively). In particular, we will be considering the action of G on left cosets of its maximal Frobenius subgroups (or their conjugates respectively). For instance, let Ω_p represent the

$|G : N_P| = r$ points upon which G acts. We may view this set in three useful, yet (permutation) equivalent, manners.

$$\Omega_p = \begin{cases} \text{the set of left cosets of } N_P \text{ in } G \text{ (action by left multiplication)} \\ \text{the set of normalizers of Sylow } p\text{-subgroups (action by conjugation)} \\ \text{the set of Sylow } p\text{-subgroups (action by conjugation)} \end{cases}$$

The stabilizer of a point in the action of G on Ω_p is $G_\alpha = N_P$. The orbits of G_α are of size

$$\begin{aligned} |G_\alpha : G_\alpha \cap G_\beta| &= |N_P : N_P \cap N_{P^x}| \\ &= p^a \quad \text{or} \quad p^a q \quad \text{respectively} \end{aligned}$$

on $\Omega_p - \{\alpha\}$. By Sylow's Theorem, $|G : N_R| = p^{a-1}q \equiv 1$ modulo r and so $p^{a-1}q > r$. The order of $\Omega - \{\alpha\}$ is $r - 1$, which must then be less than $p^a q$. Therefore there are no orbits of size $p^a q$ in the action of N_P on Ω_p. Thus every nontrivial orbit has size p^a. If there are t such orbits we may write:

$$r = 1 + tp^a.$$

Furthermore, we can consider the action of Q on each orbit of $G_\alpha = N_P$, as $N_P = PQ$. By Corollary 1.1.7, Q has a unique fixed-point on each orbit since P is a regular normal subgroup of N_P acting on an orbit; as there are $t + 1$ such orbits we have that

$$Q \text{ has } t + 1 \text{ fixed-points in its action on } \Omega_p.$$

Let π denote the permutation representation of G acting on Ω_p so that $\pi(g)$ equals the number of fixed-points of g acting on Ω_p for every $g \in G$. Although ostensibly the use of π introduces character theory into our proof, it is rather a convenient shorthand for keeping track of all the fixed points of permutations, and so could likely be avoided. In particular, $\pi(1) = r$, and $\pi(g) = 0$ for every $g \in G$ such that $|g| = r$, since no Sylow r-subgroup normalizes any Sylow p-subgroup. Also, any element g of order p can fix only one $P \in \mathrm{Syl}_P(G)$, therefore $\pi(g) = 1$.

We can summarize the value of π on the elements of G as follows:

$$\pi(g) = \begin{cases} r \quad \text{if } g = 1 \\ 1 \quad \text{if } |g| = p \\ t+1 \quad \text{if } |g| = q \\ 0 \quad \text{if } |g| = r. \end{cases}$$

Since G acts transitively on Ω_p, Corollary 3.2.7 allows us to determine that $\pi(g) = p$ for $|g| = q$ as $(1_G, \pi)_G = 1$. Therefore $p = t + 1$ and we have:

$$\text{A:} \quad r = (p-1)p^a + 1.$$

Let us now work to understand the action of N_Q (as a subgroup of G) on Ω_p. Denote a Frobenius complement of Q in N_Q as P_1; recall that this subgroup is of order p. First consider the action of Q on Ω_p. Let y be an element of order q and $x \in P_1$ where $|x| = p$. From previous discussion, y fixes exactly p points in the action of Q on Ω_p. Let $\mathcal{Q}_1$ be the p points fixed by Q. On the remaining points Q is a product of $\frac{r-p}{q}$ disjoint q-cycles. Note that x acts on the set $\mathcal{Q}_1$ of fixed-points of Q. If x fixed any point in $\mathcal{Q}_1$, then both x and Q would normalize the Sylow p-subgroup P. Since x is an element of order p normalizing P, $x \in P$. Thus $[x, Q] \leq P \cap Q = 1$, *i.e.*, x commutes with Q which is a contradiction. Thus x acts without fixed-points, hence is a p-cycle on $\mathcal{Q}_1$. However, we know that $\pi(x) = 1$ so P_1 must fix one of the remaining q-cycles (*i.e.*, not every orbit of N_Q on $\Omega_p - \mathcal{Q}_1$ can be a regular orbit for N_Q). Let $\mathcal{Q}_2$ denote the orbit of N_Q on Ω_p on which Q acts as a q-cycle, and denote the remaining elements of Ω_p as $\mathcal{Q}_3$. The points in the latter set must all lie in regular orbits for N_Q. This implies that $\mathcal{Q}_3$ can be divided into a number of N_Q orbits, say e, where each one is a sum of p blocks of size q cyclicly permuted by P_1. Thus $\mathcal{Q}_3$ is of size epq. We then have that

$$\text{B:} \quad r = |\Omega_p| = |\mathcal{Q}_1| + |\mathcal{Q}_2| + |\mathcal{Q}_3| = p + q + epq.$$

As we considered the action of G on Ω_p, the set of Sylow p-subgroups, we can also consider the action of G on Ω_r, the set of Sylow r-subgroups. The (permutation) equivalent interpretations of Ω_p can also be applied to Ω_r with the respective group action. Care needs to be taken however, because $|\Omega_r| = p^{a-1}q$, so this action of G on Ω_r is not of prime degree as in the case of G acting on Ω_p.

Consider the action of N_R on Ω_r. Recall that $N_R = RP_2$ for $|P_2| = p$. Our intention is to count the number of fixed-points of P_2 acting on Ω_r in two ways to derive another equation for r. Let us first fix Q so that $N_P = PQ$ and fix R so that R is normalized by $P_2 \leq P$.

First, by assuming that P is elementary abelian we can write $P = P_2 \times P_3$ where P_3 is an elementary abelian group of order p^{a-1}. For every $x \in P$ there exist $y \in P_2$ and $z \in P_3$ such that $x = yz$ so we have that R^x is a conjugate of R and thus represented in Ω_r. If the subgroup P_2 normalizes R^x then $P_2^{x^{-1}}$ normalizes R. This implies then that $P_2^{x^{-1}} = P_2^w$ for some $w \in R$. Therefore $wx = n \in N_G(P_2) = P$, since Q does not normalize P_2 ($|Q| > |P_2| = p$). Thus we can write $wx = yz$ for $y \in P_2$ and $z \in P_3$. Then $x = w^{-1}yz$ so

$$R^x = R^{w^{-1}yz} = R^{yz} = R^z \qquad \text{for some } z \in P^3.$$

Conversely, P_2 does normalize R_z for every $z \in P_3$, hence P_2 fixes an element of Ω_r, R^x, if and only if $R^x = R^z$ for some $z \in P_3$. Therefore

$$P_2 \text{ fixes exactly } p^{a-1} \text{ elements in } \Omega_r.$$

We can also arrive at an equation for the number of fixed-points of P_2 acting on Ω_r by dividing Ω_r into its differently sized orbits under the action by N_R. The normalizer N_R fixes R, which creates an orbit of size 1. The Frobenius kernel R fixes no other Sylow r-subgroup thus the remaining orbits must have size divisible by r. Some of these orbits will be regular orbits, consisting of pr Sylow r-subgroups permuted transitively by N_R. The remaining subgroups will fall into orbits of size r, in which P_2 will fix exactly one element (by Corollary 1.1.7). Thus we may partition Ω_r so:

$$\Omega_r = \{R\} \cup \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_d \cup \mathcal{O}_{d+1} \cdots \cup \mathcal{O}_{d+c}$$

where there are d regular orbits, each of size pr, and c nonregular orbits, each of size r. The number of fixed-points of P_2 acting on Ω_r is one more than the number of nonregular orbits, hence is $c+1$. Thus $c+1=p^{a-1}$ by the previous paragraph.

The division of Ω_r into its orbits under the action of N_R also allows for another expression of $p^{a-1}q$ in terms of p, r, c, and d as follows.

$$p^{a-1}q = 1 + dpr + cr$$

In the above equation we can replace c by $p^{a-1}-1$ to arrive at

$$p^{a-1}q = 1 + dpr + r(p^{a-1}-1) = p^{a-1}r + 1 + dpr - r.$$

We have previously established that $q < r$, so in order for the equality to hold it must be the case that $d = 0$. Thus there are no regular orbits in the action of N_R on Ω_r and we have

$$p^{a-1}q = p^{a-1}r + 1 - r.$$

We can rearrange the above equation to be $r = p^{a-1}(r-q)+1$. We then have the following three equations for r, after combining with the two established previously:

A: $r = (p-1)p^a + 1$

B: $r = p + q + epq$

C: $r = p^{a-1}(r-q) + 1$

Equations A and C tell us that $p^a(p-1) = p^{a-1}(r-q)$, so in fact $p(p-1) = r-q$. Rearranging equation B tells us that $r - q = p(1+eq)$. Therefore we have that $p(p-1) = p(1+eq)$, or in other words, $p-1 = 1+eq$. However, $q > p$ by Proposition 3.2.9, so this forces $e = 0$. In this case then, $p-1 = 1$ and so $p = 2$. This contradicts the fact that G is of odd order. Therefore a simple G under the hypotheses of this subsection cannot exist. ∎

The main result of the proof to Proposition 3.2.10 is the impression that this method of approach to showing solvability of odd order CA-groups may be too similar to Burnside's case-by-case strategy to generalize. The constraint on G that the Sylow p-subgroup be elementary abelian seems difficult to remove and still be able to produce results. We have yet to be able to generalize our results, even to a simple CA-group G of order $p^a q^b r$ for distinct primes p, q, and r and for G with elementary abelian Sylow p-subgroup. For this reason, we explored another approach – using graph theory to show nonexistence of simple odd order CA-groups.

3.3 Graph Theoretic Approaches

Graph theory is a growing field of mathematics the techniques of which have yet, to the best of our knowledge, to be employed towards simplifying the proof of Suzuki's Theorem. This section explains our recent work to incorporate some of the ideas of graph theory into a proof that a simple CA-group of order $p^a qr$ (with elementary abelian Sylow p-subgroup and three conjugacy classes of maximal Frobenius subgroups) does not exist. For this section, assume G to be a simple CA-group whose Frobenius kernels are the Sylow subgroups and where the Sylow p-subgroups are elementary abelian for p the smallest prime dividing $|G|$. Throughout this section we will be denoting the degree of a vertex v in a graph by $d(v)$. To distinguish between groups and graphs, $\mathcal{G}$ will denote a graph.

For a group G we define a set of graphs hoping to show that at least one in this set cannot exist when G is of odd order. We used A_5, $\mathrm{SL}_2(\mathbb{F}_8)$, and a hypothetical simple group G with order $3^3 \cdot 7 \cdot 13 \cdot 409$ as primary examples. In fact, this approach provides another proof that the latter group does not exist.

Definition 3.3.1. Given a group G, and a prime p such that $p \mid |G|$. Define a graph $\mathcal{G}_p$ by $\mathcal{V}_p = \{P \mid P \in \mathrm{Syl}_p(G)\}$, and $\mathcal{E}_p = \{(P_1, P_2) \mid N_G(P_1) \cap N_G(P_2) \neq 1 \text{ and } P_1 \neq P_2\}$.

A particular group G will have a graph for every prime dividing the order of G. Let us consider the graph $\mathcal{G}_2$ associated with A_5.

The group A_5 has $|A_5 : N(P)| = 5$ Sylow 2-subgroups, each of order 4. Thus the graph $\mathcal{G}_2$ has 5 vertices. With a group as small as A_5 it's possible (though tedious) to actually write out a list of the conjugates of the Sylow 2-subgroup and the elements in their normalizers to physically check for nontrivial intersections.

This brute force method shows that the $\mathcal{G}_2$ graph for A_5 is *complete*, meaning that it has every possible edge. (We shall see that the $\mathcal{G}_3$ graph for A_5 turns out to be the Peterson graph, and the graph $\mathcal{G}_5$ is a complete graph.)

We now generalize the construction of the graphs associated with a group G. For a general group G, let p be any prime dividing $|G|$. For $P \in \mathrm{Syl}_p(G)$, let $N_P = N_G(P)$ and recall $N_P = PQ$ for some subgroup Q of prime power order q^b. Let $\mathcal{V}_Q(P)$ denote

$$\mathcal{V}_Q(P) = \{P^x \in \mathcal{V}_p \mid (P, P^x) \in \mathcal{E}_p \quad \text{and} \quad N_G(P) \cap N_G(P^x) = Q\} \subseteq \mathcal{V}_p,$$

the set of conjugates of P that are "connected to P via Q." In addition, suppose that $N_Q = N_G(Q) = QS$ for some subgroup S of prime order such that $s \neq q$ (where s may or may not equal p). Finally, assume that $S \cap N_P = 1$, which is always true if S does not centralize Q.

Theorem 3.3.2. *The subgroup S acts transitively by conjugation on $\mathcal{V}_Q(P) \cup \{P\}$.*

Proof. Let $P^x \in \mathcal{V}_Q(P)$. Since $Q \leq N_G(P^x)$ we have $Q^{x^{-1}} \leq N_G(P)$. Therefore Q and $Q^{x^{-1}}$ are Sylow q-subgroups of $N_P = QP$. Since P is transitive on $\mathrm{Syl}_q(N_P)$, we obtain $Q^{x^{-1}} = Q^h$ for some $h \in P$. Now $Q^{hx} = Q$ so $hx \in N_Q = QS$. Thus $hx = yz$ for some $y \in Q$ and some $z \in S$, and so $x = h^{-1}yz$. Finally

$$\begin{aligned} P^x &= P^{h^{-1}yz} \\ &= P^{yz} \quad (h \in P) \\ &= P^z \quad (y \in Q \leq N_P) \end{aligned}$$

Conversely, if z is a nonidentity element of S then $Q = N_P \cap N_{P^z}$ and so S is transitive on $\mathcal{V}_Q(P) \cup \{P\}$. ■

Note that the hypotheses of Theorem 3.3.2 are satisfied in our examples A_5, $\mathrm{SL}_2(\mathbb{F}_8)$, and a "potential" simple CA-group of order $3^3 \cdot 7 \cdot 13 \cdot 409$. Additionally, the case considered in Section 3.2 of this chapter also satisfies the hypotheses of Theorem 3.3.2. Corollaries 3.3.3 and 3.3.4 elaborate further on the nature of $\mathcal{V}_Q(P)$.

Corollary 3.3.3. $|\mathcal{V}_Q(P)| = s - 1$.

Proof. This is immediate from the proof of Theorem 3.3.2 together with the fact that $S \cap N_P = 1$. $\blacksquare$

Corollary 3.3.4. *The number of vertices connected to P by an edge is $|P| \cdot (s-1)$.*

Proof. Note that N_P has $|P|$ distinct Sylow q-subgroups Q and each of these determines $s-1$ vertices, $\mathcal{V}_Q(P)$. Also for $Q_1 \neq Q_2$, we have that $\mathcal{V}_{Q_1}(P) \cap \mathcal{V}_{Q_2}(P) = \emptyset$ because $N_P \cap N_{P^x}$ has order 1 or q^b for any $P \neq P^x$. $\blacksquare$

If G is a simple CA-group with maximal Frobenius subgroups $N_P = PQ$ and $N_Q = QS$, where P, Q, and S are as above, then by Corollary 3.3.4 $d(v) = |P| \cdot (s-1)$ where $s = |S|$ for any $v \in \mathcal{V}_p$. Furthermore, the vertices connected to a vertex v can be characterized by the normalizers of the Sylow subgroups these vertices represent.

Definition 3.3.5. Fix $Q \in \mathrm{Syl}_q(N_P$. A *kite (of type Q)* is the subgraph of $\mathcal{G}_p$ whose vertices are $\{P\} \cup \mathcal{V}_Q(P)$ and all edges in $\mathcal{G}_p$ joining these for some $Q \in \mathrm{Syl}_q(N_P)$.

Definition 3.3.5 implies that the graph $\mathcal{G}_p$ as previously defined can be divided at any vertex into kites representing the Sylow p-subgroups normalized by the same subgroup Q. Note that by definition the size of a kite includes a "central vertex," P. So if a vertex has one kite of size 3, for example, then the degree of the vertex is 2. Corollary 3.3.6 describes the kite substructure of a graph $\mathcal{G}_p$.

Corollary 3.3.6. *A kite is a complete graph on s vertices.*

Proof. We have already shown that a kite has s vertices. For every $P^x \in \mathcal{V}_Q(P)$ we have that $N_P \cap N_{P^x} = Q$. Thus $Q \leq N_{P^x} \cap N_{P^y}$ for every $P^y \in \mathcal{V}_Q(P)$ too. This means that every pair of vertices in $\mathcal{V}_Q(P)$ are joined (by "edge Q"), as needed. $\blacksquare$

To generalize, recall that $s = |N_G(Q) : Q|$. Note also that if Q_1 and Q_2 are distinct Sylow q-subgroups of N_P then the kites of type Q_1 and type Q_2 have only the vertex P in common. This proves:

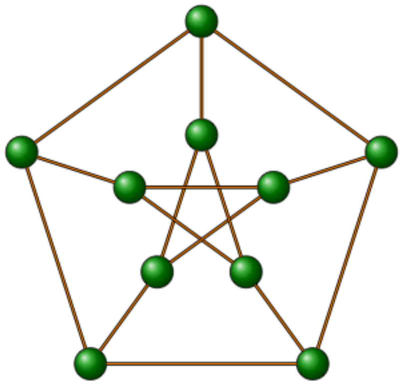

Figure 3.1: The Petersen graph.

Proposition 3.3.7. *The set of vertices of $\mathcal{V}_p$ connected to a fixed Sylow p-subgroup P is partitioned in $|P|$ disjoint subsets $\mathcal{V}_Q(P)$, one for each $Q \in Syl_q(N_P)$. In particular, the degree of $\mathcal{G}_p$ (at each vertex) is $|P| \cdot (s-1)$.*

Let us again consider the graph $\mathcal{G}_2$ associated with A_5 with these new results in mind. The normalizer of $P = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$ is $N_{A_5}(P) = P\langle (2\,3\,4) \rangle = PQ$. Recall that Q is normalized by P_0 (playing the role of S above), a subgroup of size 2 ($= s$). Thus $|N(Q) : Q| = |QP_0 : Q| = 2$ and so each kite is of size 2. There are $|P| = 4$ kites, and we see the degree of each vertex is $(2-1) \cdot 4 = 4$. With a total of 5 vertices, each of degree 4, clearly the graph is complete as previously established.

Consideration of the Sylow 5-subgroup yields a graph $\mathcal{G}_5$ with six vertices and at each vertex there are 5 kites of size 2. Thus the graph $\mathcal{G}_5$ for A_5 is also complete. The graph $\mathcal{G}_3$ is different; $\mathcal{G}_3$ has $|A_5 : N(Q)| = 10$ vertices and at each vertex there are three kites of size 2. So the degree of each vertex is $(2-1) \cdot 3 = 3$, meaning that the graph cannot be complete. In this instance, the graph is the Peterson graph [Chartrand, Figure 1.9].

We can summarize the relevant information from each graph associated with our example groups in table format. For A_5, the table is shown here as Table 3.1. If the degree of each vertex in a graph is one less than the total number of vertices then the graph is complete, as seen in $\mathcal{G}_2$ and $\mathcal{G}_5$ associated with A_5. Thus the

prime	2	3	5
size of normalizer	$2^2 \cdot 3$	$3 \cdot 2$	$5 \cdot 2$
# vertices	5	10	6
# kites	4	3	5
size of kites	2	2	2
$d(v)$	4	3	5

Table 3.1: Summary of the graphs $\mathcal{G}_p$ for A_5.

prime	2	3	7
size of normalizer	$2^3 \cdot 7$	$3^2 \cdot 2$	$7 \cdot 2$
# vertices	9	28	36
# kites	8	9	7
size of kites	2	4	4
$d(v)$	8	27	21

Table 3.2: Summary of the graphs $\mathcal{G}_p$ for $\mathrm{SL}_2(\mathbb{F}_8)$.

only graph associated with A_5 that is not complete is $\mathcal{G}_3$. Recall that a Sylow 2-subgroup is normalized by a Sylow 3-subgroup. This coincidence is repeated again in the graphs associated with $\mathrm{SL}_2(\mathbb{F}_8)$. There are again three primes dividing the order of $\mathrm{SL}_2(\mathbb{F}_8)$, this time a Sylow 7-subgroup normalizes a Sylow 2-subgroup. Below is a summary of the three graphs for $\mathrm{SL}_2(\mathbb{F}_8)$. The graphs $\mathcal{G}_2$ and $\mathcal{G}_3$ are complete, but the graph $\mathcal{G}_7$ is not; each vertex is connected to exactly 21 other vertices, but not the remaining 15.

While the coincidence of the graph associated with the prime normalizing the elementary abelian Sylow subgroup of G not being complete is interesting, the fact is that A_5 and $\mathrm{SL}_2(\mathbb{F}_8)$ are fundamentally different from a hypothetical simple CA-group G of odd order and the graphs associated with G should reflect this.

Consider the graphs of a hypothetical minimal simple CA-group G of order $3^3 \cdot 7 \cdot 13 \cdot 409$. The graphs for this group demonstrate that the information from A_5 and $\mathrm{SL}_2(\mathbb{F}_8)$ are quite different from this configuration. There is an immediate contradiction in the graph $\mathcal{G}_{409}$ associated with G. This graph has $3^2 \cdot 7 \cdot 13 = 819$ vertices, but any one vertex $v \in \mathcal{G}_{409}$ has degree $d(v) = 8 \cdot 409 = 3272$. This strikes

prime	3	7	13	409
size of normalizer	$3^3 \cdot 13$	$7 \cdot 3$	$13 \cdot 3$	$409 \cdot 3$
# vertices	$7 \cdot 409$	$3^2 \cdot 13 \cdot 409$	$3^2 \cdot 7 \cdot 409$	$3^2 \cdot 7 \cdot 13$
# kites	3^2	7	13	409
size of kites	3	9	9	9
$d(v)$	$2 \cdot 3^3$	$8 \cdot 7$	$8 \cdot 13$	$8 \cdot 409$

Table 3.3: Graphs associated with a simple CA-group G of order $3^3 \cdot 7 \cdot 13 \cdot 409$.

prime	p	q	r
size of normalizer	$p^a q$	qp	rp
# vertices	r	$p^{a-1}r$	$p^{a-1}q$
# kites	p^a	q	r
size of kites	p	p^{a-1}	p^{a-1}
$d(v)$	$p^a(p-1)$	$q(p^{a-1}-1)$	$r(p^{a-1}-1)$

Table 3.4: Graphs associated with a minimal simple CA-group G of order $p^a qr$.

a strong resemblance to the proof that the group doesn't exist using permutation representations, which is based on G's permutation action on $\mathrm{Syl}_{409}(G)$.

We present here the descriptives of the graphs associated with a group G of order $p^a qr$, as calculated in Subsection 3.2.2. Clearly in the $\mathcal{G}_q$ graph the degree of any vertex is $(p^{a-1}-1)q$ which is less than the total number of vertices, $p^{a-1}r$, since in Section 3.2 it was established that $q < r$. Therefore that graph is not complete but no immediate contradiction is reached as in the previous example. However, in the graph $\mathcal{G}_r$ we have that the degree of any vertex, $(p^{a-1}-1)r$, should be less than the number of vertices, $p^{a-1}q$. It isn't clear that this is always the case; in some instances where r and q are close there might be a contradiction.

While the information in Table 3.4 is promising, there is no transparent contradiction. To add more constraints to the picture, we introduce Theorem 3.3.8.

Theorem 3.3.8. *Given a graph $\mathcal{G}$ with edge set $\mathcal{E}$ and vertex set $\mathcal{V}$. If $d(v)$ denotes the degree of a vertex v then*

$$\sum_{v \in \mathcal{V}} d(v) = 2|\mathcal{E}|.$$

Theorem 3.3.8 is completely elementary and is proven in [3, Theorem 1.1.1].

The equation in Theorem 3.3.8 is powerful, and will be used to provide another proof that a simple CA-group G of odd order $p^a qr$ with an elementary abelian Sylow p-subgroup and three classes of maximal Frobenius subgroups does not exist.

Proposition 3.3.9. *Under the hypotheses above, no simple CA-group G of odd order $p^a qr$ exists.*

Proof. Assume that such a group G does exist. The propositions of Section 3.2 clearly lay out the Sylow subgroup structure G must follow. We compute each side of the equation in Theorem 3.3.8 using a different technique. Let P be a Sylow p-subgroup of G and fix $Q \in \mathrm{Syl}_q(G)$ so that $N_G(P) = PQ$. Then fix $R \in \mathrm{Syl}_r(G)$ so that $N_G(R) = RP_0$ for $P_0 \leq P$ where $|P_0| = p$. In the graph $\mathcal{G}_r$ associated with G the degree of each vertex $v \in \mathcal{V}_r$ is given by $d(v) = r \cdot (|N_G(P_0) : P_0| - 1)$. Since each vertex is of the same degree we can write the sum of degrees as $|G : N_G(R)| \cdot r \cdot (|N_G(P_0) : P_0| - 1) = p^{a-1}q \cdot r \cdot (p^{a-1} - 1)$.

We now count up the number of edges using permutation group theory. The number of edges is equal to the number of kites times the size of each kite. Each vertex v in a kite represents a Sylow r-subgroup normalized by the same P_0 in the action of G on Ω_r, the set of Sylow r-subgroups of G. Thus the size of each kite equals the number of fixed-points of P_0 in the action on Ω_r. In Subsection 3.2.2, we determined the number of fixed points of P_0 to be p^{a-1}, by considering the action of $N_G(R)$ on the set of Sylow r-subgroups. Therefore $2 \cdot |\mathcal{E}_r| = 2 \cdot p \cdot p^{a-1}$.

Theorem 3.3.8 then asserts that

$$p^{a-1}qr(p^{a-1} - 1) = 2p^a.$$

On both sides of this equation cancel a factor of p^{a-1}, leaving $2p = qr(p^{a-1} - 1)$. Since p, q, and r are odd primes there is a clear contradiction. This therefore shows that a simple CA-group of order $p^a qr$ with elementary abelian Sylow p-subgroups and three conjugacy classes of maximal Frobenius subgroups does not exist, as its graph $\mathcal{G}_r$ does not exist. ∎

This is a novel method for demonstrating that a minimal simple odd order CA-group does not exist. We have not yet generalized this method from the case where the Frobenius kernels of a simple odd order CA-group G are its Sylow subgroups, but the elementary proof in the case of a simple CA-group of order $p^a qr$ for distinct primes p, q, and r and where the Sylow p-subgroup of G is elementary abelian is promising.

Chapter 4

Conclusions

If Suzuki's proof of the CA-theorem could be simplified then perhaps some of the proofs following in the Classification process could also be clarified – in particular, there could be direct effects on Feit and Thompson's proof that every odd order group is solvable. In his 2001 paper [10], R. Solomon wrote "I compare the character theory (in Chapters 3 and 5) [in the proof of the Feit-Thompson Theorem] to Bach's B Minor Mass, the glorious summation of everything which had been achieved by Frobenius, Brauer, Suzuki, and Feit himself." It's difficult to imagine simplifying such a masterful proof, but one of the cornerstones of this proof *is* Suzuki's CA-paper. Perhaps by developing new approaches to Suzuki's work, there can be additional consequences in Feit and Thompson's work or even beyond into the other parts of the Classification. This thesis has thus focused on developing new approaches to Suzuki's CA-group proof, with success in a very limited case.

In the case of a simple CA-group G of order p^aqr with p, q, and r distinct odd primes and the Sylow p-subgroup elementary abelian, the prime r plays a very important role in proving that such a group cannot exist. The crux of our proof relies on the fact that the normalizer of a Sylow p-subgroup has prime index, r, and so we can eke out several ways in which to express r in terms of the other primes. However, the moment the order is generalized to $p^aq^br^c$ or even p^aq^br, this advantage is lost since it's not readily possible to show that any maximal Frobenius subgroup has prime index. Thus generalizing further to any odd order

CA-group with three conjugacy classes of Frobenius subgroups is a daunting task. Also, there are no CA-groups with four conjugacy classes of Frobenius subgroups, even among the simple even order CA-groups. This begs the question, Is there an obvious way to prove the nonexistence of odd order CA-groups with four conjugacy classes of maximal Frobenius subgroups without using character theory, thereby greatly simplifying Suzuki's CA-proof? The cases of a simple CA-group with order $3^3 \cdot 7 \cdot 13 \cdot 409$ and of a simple CA-group with order $3^7 \cdot 13 \cdot 41 \cdot 547 \cdot 1093 \cdot 4493$ suggest that among simple CA-groups with four conjugacy classes of maximal Frobenius subgroups, permutation group theory may be a good avenue down which to explore for proofs of nonexistence.

The graph theoretic method developed in Section 3.3 is very efficient in showing that our particular $p^a qr$ case of a CA-group does not exist. There was also a very promising immediate contradiction in the graphs associated with a hypothetical simple CA-group of order $3^3 \cdot 7 \cdot 13 \cdot 409$. However, we have yet to extend the definition of the graph to CA-groups with a conjugacy class of Frobenius kernels that is not represented by a Sylow subgroup. Such an extension might provide an elementary means of showing that such groups do not exist.

During the development of our new Burnside number we surmised that one of the primes would be 547 since it is equal to $\frac{1093+1}{2}$. Can a method be developed to discover hypothetical simple CA-groups with five or more conjugacy classes of maximal Frobenius subgroups? With more examples of "possible" orders of odd order simple CA-groups come more opportunities to develop methods of proof of their nonexistence – one such method might be able to generalize. It would be helpful to have a few examples of simple CA-groups whose Frobenius kernels are not Sylow subgroups, even if these examples are hypothetical since any insight regarding the manner in which to prove that such groups of odd order do not exist would be useful.

The work conducted in this thesis is by no means complete. We have discovered a new Burnside number and begun to develop a graph theoretic proof that may extend to show a particular family of simple CA-groups (those with Sylow subgroups as maximal Frobenius kernels) does not exist. We have also produced a permutation group theoretic proof that a specific kind of odd order simple CA-group does not exist. While we have made some progress towards developing new methods that might be helpful in simplifying Suzuki's CA-proof, we have yet to generalize our methods to be able to deal with a wider range of CA-groups.

Bibliography

[1] N. L. Biggs and A. T. White. *Permutation Groups and Combinatorial Structures.* Cambridge University Press, 1979.

[2] William Burnside. *Theory of Groups of Finite Order.* Dover Publications, Inc., 1955.

[3] G. Chartrand and L. Lesniak. *Graphs and Digraphs.* Chapman and Hall/CRC, 1996.

[4] David S. Dummit and Richard M. Foote. *Abstract Algebra, Third Edition.* John Wiley & Sons, Inc., 2004.

[5] Walter Feit. *Characters of Finite Groups.* W. A. Benjamin, Inc., 1967.

[6] Walter Feit and John G. Thompson. Solvability of groups of odd order. *Pacifical Journal of Mathematics*, 13(3):775 – 1092, 1963.

[7] Daniel Gorenstein. *Finite Groups.* Harper - Row, 1968.

[8] B. Huppert. *Endliche Gruppen I.* Springer, 1967.

[9] Donald S. Passman. *Permutation Groups.* W. A. Benjamin, Inc., 1968.

[10] Ronald Solomon. A brief history of the classification of the finite simple groups. *Bull. A.M.S.*, 38(3):315 – 352, 2001.

[11] Michio Suzuki. The nonexistence of a certain type of simple groups of odd order. *Proc. A.M.S.*, 8:686 – 695, 1957.

[12] Michio Suzuki. *Group Theory I.* Springer-Verlag New York Inc., 1982.

[13] Michio Suzuki. *Group Theory II.* Springer-Verlag New York Inc., 1986.