SOLVABLE GROUPS WHOSE CHARACTER DEGREE GRAPHS HAVE DIAMETER THREE

A dissertation submitted to Kent State University in partial fulfillment of the requirements for the degree of Doctor of Philosophy

by

Carrie T. Dugan

August, 2007
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Related Results</td>
<td>6</td>
</tr>
<tr>
<td>Construction</td>
<td>21</td>
</tr>
<tr>
<td>Bilinear Forms</td>
<td>28</td>
</tr>
<tr>
<td>Commutators</td>
<td>40</td>
</tr>
<tr>
<td>Irreducible Characters Part I</td>
<td>52</td>
</tr>
<tr>
<td>Irreducible Characters Part II</td>
<td>56</td>
</tr>
<tr>
<td>Irreducible Characters Part III</td>
<td>60</td>
</tr>
<tr>
<td>A Specific Example</td>
<td>68</td>
</tr>
<tr>
<td>Irreducible Characters Part IV</td>
<td>75</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

There are many people that deserve recognition for my ability to complete my dissertation. I would like to begin by thanking my family. My husband gave me the strength to persevere and the support to make it all come to fruition. He kept me grounded when times were difficult. This could not have been completed without his love and devotion to my dream.

There are others in my family who also stood by me throughout graduate school. My parents were two of my biggest cheerleaders for the duration. My father finished his doctoral work when my siblings and I were young. So he and my mother knew how hard it was for me to do graduate work with children at home. My father knew how difficult my work would be and my mother knew how difficult my husband’s work would be. Knowing this helped me finish what I started.

I want to thank Steve Gagola for being a mentor during my years at graduate school. I took abstract algebra from Dr. Gagola my first year at Kent State University. He made the course exciting and interesting and is one of the main reasons I chose to pursue research in group theory.

Finally, there are not enough words to express my gratitude toward my advisor, Mark Lewis. I would not have survived the intensity of the program without his guidance. He became more of a mentor than I thought was possible. I could always count on him to make time for me and to answer the many questions I had. He is not only someone I admire tremendously. He is my lifelong friend.
CHAPTER 1

INTRODUCTION

In a broad sense, character theory is an alternative way to study finite groups. The \textit{characters} of a finite group $G$ are functions, $\chi$, from $G$ to the complex numbers. A representation of a group lets us think of the group in terms of matrices, and characters are defined by the trace of a representation of $G$. The value of a function of this type at $1 \in G$ is known as the \textit{character degree}, or degree of $\chi$. The \textit{irreducible} characters of $G$, denoted $\text{Irr}(G)$, are the characters arising from the irreducible representations of $G$. Our focus is on irreducible characters and their degrees. Within a finite group, the conjugacy classes partition the group and the number of irreducible characters of $G$ is equal to the number of conjugacy classes of $G$. More on conjugacy classes can be found in the next chapter. The set of all irreducible character degrees is the set $\text{cd}(G) = \{ \chi(1) \mid \chi \in \text{Irr}(G) \}$.

We define the set of vertices, $\rho(G)$, to be the set of all primes that divide degrees in $\text{cd}(G)$. The \textit{character degree graph}, or degree graph, $\Delta(G)$, associated with $\text{cd}(G)$ obtains its vertices from the set $\rho(G)$. Within $\Delta(G)$ we have an edge connecting $p, q \in \rho(G)$ if $pq$ divides some degree $a \in \text{cd}(G)$. The distance between two vertices in a graph is the minimum number of edges in any path joining those two points. The \textit{diameter} of $\Delta(G)$ is defined to be the maximum distance between any two vertices. A graph is \textit{connected} if there is a path from every vertex in $\rho(G)$ to every other vertex. In a disconnected graph we typically characterize each connected component of the
It is known that in a solvable group the number of connected components is at most two. This was shown in [12]. Corollary 4.5 of [13] tells us that if $G$ is a solvable group and $\Delta(G)$ is disconnected, at least one connected component of $\Delta(G)$ is a complete graph and the other connected component has diameter at most two. We mention that it appears that Pálfy was the first to prove that in a solvable group $G$, if $\Delta(G)$ is disconnected, then each connected component is a complete graph. Thus, in this case, the diameter is one. The graph of the group we will construct has diameter three, and thus, is only relevant to the case when $\Delta(G)$ is connected.

A very important and very relevant characterization of a character degree graph of a solvable group is known as Pálfy’s condition. In [15], Pálfy proved that any solvable group has the property that any three primes in $\rho(G)$ must have an edge in $\Delta(G)$ that is incident to two of those vertices. We say that a graph satisfies Pálfy’s condition if it has this property. It turns out that connected graphs satisfying Pálfy’s condition have diameter at most three. This was proven true by Manz, Willems, and Wolf in [13]. Following this result, Huppert [3] conjectured that the diameter of $\Delta(G)$ was at most two in the case of a solvable group $G$ with one connected component. At the time of his conjecture, there were no known examples where the diameter of $\Delta(G)$ was three. All that was known was that the diameter had a bound of three. This is the origin of the work done by Lewis in [9].

The problem solved in this paper began as a conjecture by Lewis in [9], that the type of group he constructed could be generalized to produce a degree graph with diameter three. Thus, we saw the possibility of a family of groups whose structure was the same as, or similar to that of the group in [9] and in particular, whose character
degree graph has diameter three. We began to think of the result in [9] in more
general terms with the goal in mind of constructing a similar family of groups whose
character degree graphs yielded a diameter of three.

In [9], Lewis showed that a solvable group whose character degree graph has
diameter three does exist. In the construction of the group he used specific primes,
\( p = 2, q = 3, \) and \( r = 5, \) which produced a degree graph having diameter three. Here
we generalize that idea and choose any prime \( p, \) and primes \( q \) and \( r, \) which will have
certain divisibility conditions placed upon them. These conditions will be outlined in
Chapter 3 when we detail the construction of our group.

The main algebraic structure of our group is that of the group in [9]. However, as
we began working on this result, it became very apparent that with \( q > 3, \) the group
takes on a much more complicated structure. Many things become complicated when
\( q > 3. \) If we had instead fixed \( q = 3 \) and chosen \( p = 2 \) and \( r \) with the appropriate
parameters, we could have mimicked the result in [9]. Even if we let \( p \) be any prime
and fix \( q = 3, \) the proof and techniques of proving are not that different from the case
of Lewis. Thus, the real work involved in this problem lies in the case when \( q > 3. \)

The techniques used in [9] can be used here, however, only up to those results
needed to prove the general \( q = 3 \) case. In fact, this specific case is summarized in
Chapter 9. Only a couple of minor points needed to be changed from those of Lewis
in Chapter 9. The majority of the work comes when we move beyond this case.

One purpose of the restrictions placed on \( p, q, \) and \( r \) is to ensure coprime group
actions, which brings us to the point that the conditions we have set on our primes
are essentially those used in [6]. Also, the construction of our group is the same con-
struction Lewis used, which can be found in [6]. The main result in [6] characterizes
the derived subgroup of a group that is being acted on coprimely as nilpotent, hence
solvable. Our interest was not this, necessarily, but the construction of the group in addition to the results on coprime actions.

A relevant result is Lemma 4.1 in [6]. In short, Isaacs characterizes a particular type of commutator. We devote the entire Chapter 5 of this paper to commutators because understanding the commutators of certain elements within our group is essential to the end result here. Much of the work involved in this paper sits inside Chapter 5. Though Lemma 4.1 in [6] is helpful in a few instances, it is not enough to characterize all of the commutators we are interested in. There is more on the definition of the commutator of two elements and why they are such an integral part of our main goal in Chapters 2 and 5.

Arguably, one of the most helpful results in attaining our goal here is Theorem 4.4 in [16]. Riedl also constructed a group using construction techniques similar to those of Isaacs. In [16], he focused on calculating character degrees of a particular class of \( p \)-groups. As the reader will see in Chapter 3, within our group lies this same class of \( p \)-groups. Thus, we rely heavily on Theorem 4.4 in [16].

As we set out to prove our group had diameter three, we knew from previous results of others that we would have a minimum of six vertices in our graph. To see this, notice that a graph with diameter three must have \( |\rho(G)| \geq 4 \). Zhang proved in [17] that there does not exist a solvable group with four vertices and diameter three. In [10], Lewis showed the case of five vertices and diameter three does not occur. Therefore, we knew \( |\rho(G)| \geq 6 \). In general, we expected the cardinality of \( \rho(G) \) to be larger than six. The group constructed in [9] is somewhat rare, since \( \frac{p^q-1}{p-1}, \frac{p^r-1}{p-1}, \) and \( \frac{(p^q-1)(p-1)}{(p^r-1)(p^q-1)} \) turned out to be 7, 31, and 151, which are all prime numbers.

As expected, it is possible to have more than six vertices with this family of groups, depending on the the primes used. What occurs, however, is that there are certain
‘families’ of primes within $\rho(G)$ that form complete graphs and for all intents and purposes can each be thought of as one vertex, since the diameter of a complete graph is one. Thus, in reality, a group of this type will more than likely have $|\rho(G)|$ larger than six, but because of the nature of this set we still have a graph with diameter three. In particular, our graph is isomorphic to the graph in [9].
This Chapter is in place to provide the general reader with enough background to better understand the results in this paper. All of these results are well known among group theorists, who may wish to skip to the next chapter. We provide the information in this chapter without proof. The majority of the results provided can be found in [7] and [5].

We begin this chapter with one of the most fundamental results in group theory, the First Isomorphism Theorem. The main idea to extract from this theorem is that the normal subgroups of any group can be found in the manner outlined. They are in fact, kernels of homomorphisms between groups.

**Theorem 2.1 (First Isomorphism)** Let $G$ and $H$ be groups, let $\varphi : G \longrightarrow H$ be a surjective homomorphism and let $N = \ker(\varphi)$. Then $H \cong G/N$. In fact, there exists a unique isomorphism $\theta : G/N \longrightarrow H$ such that $\pi \theta = \varphi$, where $\pi$ is the canonical homomorphism from $G$ to $G/N$.

The next theorem is equally as important as the First Isomorphism Theorem. When two groups are isomorphic they are essentially ‘equal’ in the sense that they share group theoretic properties, as the next theorem tells us.
Theorem 2.2 (Correspondence) Let $\varphi : G \to H$ be surjective homomorphism and let $N = \ker(\varphi)$. Define the following set of subgroups:

$$S = \{ U \mid N \leq U \leq G \} \text{ and } T = \{ V \mid V \leq H \}.$$ 

Then $\varphi(\cdot)$ and $\varphi^{-1}(\cdot)$ are inverse bijections between $S$ and $T$. Furthermore, these maps respect containment, indices, normality and factor groups.

With the Isomorphism Theorems at hand we can mention another well-known theorem that is used to help understand the structure of the group. Within the structure of the group we construct here, for that matter many groups, lie what are called diamonds. It is always extremely helpful to be able to find isomorphic subgroups within a group to determine part of the structure of the group. In other words, we know that isomorphic groups share group theoretic properties. Thus, if we can find a group, or a subgroup that is isomorphic to a group in which we know the structure, then we answer many questions.

Theorem 2.3 (Diamond) Let $N \triangleleft G$ and $H \subseteq G$. Then $H \cap N \triangleleft H$ and $H/(H \cap N) \cong NH/N$.

Group actions help us count elements in a finite group since, for one thing, the orbits partition the group. One very important tool used relative to group actions and counting elements is the Fundamental Counting Principle (FCP). In order to show the FCP, we need to mention the stabilizer of an element. Let $G$ act on the set $\Omega$ and $\alpha \in \Omega$. We define the stabilizer of $\alpha$ to be $G_\alpha = \{ g \in G \mid \alpha \cdot g = \alpha \}$. As an example, a very common group action is conjugation. Conjugation is given by $\alpha^g = g^{-1}\alpha g$. It is clear that for $g$ to stabilize $\alpha$ we must have $g^{-1}\alpha g = \alpha$ so that the stabilizer of $\alpha$
will be the centralizer of $\alpha$ in $G$, written $C_G(\alpha)$. The following theorem, Theorem 4.9 in [7], leads directly into the FCP. Thus, it is worth mentioning.

**Theorem 2.4** Let $G$ act on $\Omega$ and let $O$ be an orbit of this action. Let $\alpha \in O$ and write $H = G_\alpha$ for the stabilizer. Then there exists a bijection $O \leftrightarrow \{Hx \mid x \in G\}$.

In other words, Theorem 2.4 says that there is a bijection between the elements of an orbit of the action and the right cosets of a stabilizer. We write the FCP as a corollary to Theorem 2.4, as was done in [7].

**Corollary 2.5** Suppose $G$ acts on $\Omega$, and let $O$ be an orbit. Then $|O| = |G : G_\alpha|$, where $\alpha$ is any element of $O$. If $G$ is finite, we have $|O| = |G|/|G_\alpha|$, and in particular, $|O|$ divides $|G|$.

A corollary and an application of the FCP relative to conjugation that is important to character theory needs mentioning. Conjugation is a very common group action that is used and happens to be related to many results in character theory. One of the most important results related to this within character theory is that the number of conjugacy classes of a finite group is equal to the number of irreducible characters.

**Corollary 2.6** Let $g \in G$ and let $cl(g)$ denote the conjugacy class containing $g$. Then $|cl(g)| = |G : C_G(g)|$. In particular, for a finite group, all class sizes divide the order of the group.

Suppose $H, N$ are groups, and $H$ acts on $N$ via automorphisms. An action of this type means that for all $x, y \in N$ and $h \in H$, we have $(xy) \cdot h = (x \cdot h)(y \cdot h)$. A very useful result arises when $\gcd(|N|, |H|) = 1$ and $N$ is abelian. This result is known as Fitting’s Lemma. Before we state Fitting’s Lemma we mention a couple of definitions.
If $N$ and $H$ are groups, the **commutator group** generated by $N$ and $H$, denoted $[N, H]$, is defined to be the group generated by the set of all $[n, h] = n^{-1}h^{-1}nh$, where $n \in N$ and $h \in H$. A subgroup $H \subseteq G$ is **characteristic** in $G$ if $\theta(H) = H$ for every automorphism $\theta$ of $G$.

**Lemma 2.7 (Fitting)** Let $H$ act on $N$ by automorphisms. Assume $\gcd(|N|, |H|) = 1$ and $N$ is abelian. Then the following hold:

1. $N = C_N(H) \times [N, H]$.

2. If $H$ and $N$ are subgroups of a group $G$, with $N \lhd G$, $G = HN$, and the given action of $H$ on $N$ being conjugation within $G$, then $G = C_N(H) \times H[N, H]$.

3. If $G$ is as in 2, then $C_N(H)$ and $[N, H]$ are characteristic subgroups of $G$.

The family of groups that we construct in this paper are **solvable** groups. So, we give the definition of a solvable group and a few group theoretic results related to this type of group. A group $G$ is solvable if there exists a finite collection of subgroups $G_0, G_1, \ldots, G_n$ such that

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

and $G_{i+1}/G_i$ is abelian for $0 \leq i \leq n - 1$. Abelian groups are automatically solvable since $G$ and 1 satisfy the definition.

Two more useful results related to group actions and solvable groups are Glauberman’s Lemma and the corollary to it. These results involve **transitive** actions. Suppose $G$ acts on $\Omega$. We say that the action is transitive if for every two elements $\alpha, \beta \in \Omega$, there exists an element $g \in G$ such that $\alpha \cdot g = \beta$. 
Lemma 2.8 (Glauberman) Let $H$ and $N$ be groups and suppose $H$ and $N$ act on $\Omega$. Also, assume that $H$ acts on $N$ via automorphisms. Suppose these actions are related by $(\alpha \cdot x) \cdot h = (\alpha \cdot h) \cdot x^h$ for $\alpha \in \Omega, h \in H$, and $x \in N$. If $N$ acts transitively on $\Omega, \gcd(|N|, |H|) = 1$, and at least one of $H$ or $N$ is solvable, then $H$ fixes some point of $\Omega$.

Corollary 2.9 Let $H, N$, and $\Omega$ satisfy the hypotheses of Glauberman’s Lemma. Then the set of $H$-fixed points of $\Omega$ forms an orbit under the action of $C_N(H)$.

In addition to the above definition of solvability, we can also think of solvability in terms of derived subgroups, or commutator subgroups. The derived subgroup $G'$ of a group $G$ is the subgroup generated by all commutators $[x, y] = x^{-1}y^{-1}xy$ for $x, y \in G$. Now, we can define $G^{(2)} = G'' = (G')'$ and in general $G^{(n)} = (G^{(n-1)})'$ for $n > 0$. The series of subgroups $G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots$ is the derived series of $G$. This leads to Theorem 8.3 in [7].

Theorem 2.10 A group $G$ is solvable if and only if $G^{(n)} = 1$ for some $n$. Also, subgroups and factors groups of solvable groups are solvable.

In the context of Theorem 2.10, the smallest integer $n$ such that $G^{(n)} = 1$ is called the derived length. We now state Corollary 8.5 of [7], as it is relevant to understanding some of the structure of our group.

Corollary 2.11 Let $1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_n = G$ be a composition series for $G$ (each factor $N_{i+1}/N_i$ is a simple group for $0 \leq i < n$). Then $G$ is solvable if and only if the composition factors $N_{i+1}/N_i$ all have prime order.

A Sylow $p$-subgroup of a finite group $G$ is defined to be a subgroup whose order is $p^a$, where $p^a$ is the full power of $p$ dividing the order of $G$. The set of all Sylow
$p$-subgroups of $G$ is denoted $\text{Syl}_p(G)$. There are three main theorems attributed to Sylow, not the least of which states that these subgroups exist in every finite group. For our purposes, however, we mention that these theorems can be found in chapter 5 of [7] and state Corollaries 5.9 and 5.10 from [7].

**Corollary 2.12** Let $G$ be finite and let $P \in \text{Syl}_p(G)$. Then $|\text{Syl}_p(G)| = |G : N_G(P)|$, and in particular, this divides $|G : P|$.

**Corollary 2.13** Let $S \in \text{Syl}_p(G)$. The following are equivalent:

1. $S \triangleleft G$.

2. $S$ is the unique Sylow $p$-subgroup of $G$.

3. Every $p$-subgroup of $G$ is contained in $S$.

4. $S$ is characteristic in $G$.

It is important for the reader to have a basic background on a special type of group, called a *Frobenius Group*. Here we provide some definitions, as well as results, involving Frobenius groups and Frobenius group actions. The best resource for more information on Frobenius groups is [2].

Given a finite group $G$, let $H \leq G$ with $1 < H < G$. Assume that whenever $g \in G - H$, we have $H \cap H^g = 1$. Then $G$ is a *Frobenius group* with respect to $H$ and $H$ is the *Frobenius complement*.

**Theorem 2.14** (*Frobenius*) Let $G$ be a Frobenius group with Frobenius complement $H$. Then the set, $N$, of all elements of $G$ not conjugate to an element of $H - 1$, satisfies (i) $N$ is a normal subgroup of $G$, (ii) $G = NH$, and (iii) $N \cap H = 1$. 
Theorem 2.14 guarantees the existence of the normal subgroup $N$. The subgroup $N$ in Theorem 2.14 is called the Frobenius kernel. Notice that $N$ can be found in the Frobenius group $G$ by setting $N = (G - \cup_{g \in G} H^g) \cup \{1\}$. It is also clear that the size of the Frobenius kernel is equal to the index of $H$ in $G$. Thus, $N$ is uniquely determined by $H$. It should be clear that all normal subgroups of $G$ that trivially intersect $H$ are contained in the kernel $N$.

An alternative definition to the one above is to say that a finite group $G$ is a Frobenius group with Frobenius kernel $N$ if $N$ is a proper, nontrivial normal subgroup of $G$ and $C_G(n) \leq N$ for all elements $n \neq 1$ of $N$. This definition, plus the above results, can be summarized in the following lemma, which is actually problem 7.1 in [5].

**Lemma 2.15** Let $N \triangleleft G$, $H \leq G$, with $NH = G$ and $N \cap H = 1$. Then the following are equivalent:

1. $C_G(n) \leq N$ for all $1 \neq n \in N$;
2. $C_H(n) = 1$ for all $1 \neq n \in N$;
3. $C_G(h) \leq H$ for all $1 \neq h \in H$;
4. every $x \in G - N$ is conjugate to an element of $H$;
5. if $1 \neq h \in H$, then $h$ is conjugate to every element of $Nh$;
6. $H$ is a Frobenius complement in $G$.

Galois theory is another very important topic in group theory that deserves to be discussed. Part of the construction of our group involves a Galois group, which we define here. Suppose $F \leq E$ is a field extension with $| E : F | < \infty$. The set
of $F$-automorphisms of $E$ is the set of all automorphisms of $E$ that fix all elements of $F$. This set is a subgroup of $\text{Aut}(E)$ and is called the Galois group of $E$ over $F$. We denote this group by $\text{Gal}(E/F)$. An extension of fields $F \leq E$ is a Galois extension if $|E : F| < \infty$ and $\text{Fix}(\text{Gal}(E/F)) = F$, where $\text{Fix}$ is defined by, $\text{Fix}(H) = \{ \alpha \in E \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H \leq \text{Aut}(E) \}$. $\text{Fix}(H)$ is a subfield of $E$ and is called the fixed field of $H$. Galois theory is used as an aid in constructing groups from fields. The following theorem is widely known as the Fundamental Theorem of Galois theory. It tells us that there is a correspondence between the subgroups of the Galois group and the intermediate fields of $E$.

**Theorem 2.16** Let $F \leq E$ be a Galois extension with $G = \text{Gal}(E/F)$. Write

$$\mathcal{F} = \{ K \mid F \leq K \leq E, K \text{ a field} \} \text{ and } \mathcal{G} = \{ H \mid H \leq G \}.$$ 

1. The maps $f(\cdot) = \text{Fix}(\cdot)$ and $g(\cdot) = \text{Gal}(E/\cdot)$ are inclusion reversing inverse bijections between $\mathcal{F}$ and $\mathcal{G}$.

2. If $g(K) = H$, then $|E : K| = |H|$ and $|K : F| = |G : H|$. In particular, $|E : F| = |G|$.

3. If $g(K) = H$ and $\sigma \in G$, then $g(\sigma(K)) = H^\sigma$, the conjugate of $H$ by $\sigma$ in $G$.

   Also, $H \triangleleft G$ if and only if $K$ is Galois over $F$, and in this case, $\text{Gal}(K/F) \cong G/H$.

Another result needed for our work in this paper is Theorem 21.10 in [7]. As the reader will see in Chapter 3, our Galois group is cyclic, as is determined by the next theorem. To be a cyclic group means that the entire group is generated by some element within the group.
**Theorem 2.17** Let $F \leq E$ be finite fields with $|F| = q$, a prime power. Then $E$ is Galois over $F$ and $G = \text{Gal}(E/F)$ is cyclic. In fact, $G = \langle \sigma \rangle$, where $\sigma : E \rightarrow E$ is defined by $\sigma(\alpha) = \alpha^q$ for $\alpha \in E$.

We mention briefly that finite fields are typically called *Galois fields* and the Galois field with $q$ elements is denoted $\text{GF}(q)$, where $q$ is any prime power. The next three results about Galois fields are Theorem 21.7 and Corollaries 21.8 and 21.9 from [7]. Additional information on finite fields can be found in Chapter 21 of [7].

**Theorem 2.18** Let $E = \text{GF}(q^n)$, where $q$ is a prime power. If $m \geq 1$ is an integer, then the following are equivalent.

1. $E$ has a subfield of order $q^m$.
2. $m$ divides $n$.
3. $q^m - 1$ divides $q^n - 1$.

According to Theorem 2.18, we now have a very useful tool to find certain subfields within a particular finite field. This fact will be used in the construction of our group, as well as the determination of certain character degrees. The following corollary also aids in determining subfields.

**Corollary 2.19** Let $E, F \leq L$ be fields, where $|E| = q^n$ and $|F| = q^m$ for some prime power $q$. Then $|E \cap F| = q^d$ where $d = \gcd(m, n)$. In particular, $F \leq E$ if and only if $m|n$.

We end this series of results on finite fields with a corollary that is used to determine all subfields of a finite field.
Corollary 2.20 Let $F \leq E$ be fields with $|F| = q < \infty$ and $|E : F| = n < \infty$. Then for each divisor $m$ of $n$, there exists a unique subfield $K$ with $F \leq K \leq E$ and such that $|K| = q^m$. There are no other intermediate fields between $F$ and $E$.

Part of the construction of our group involves rings and ideals. So, we turn our attention briefly to related ring theory and definitions. Since a ring forms an abelian group with respect to addition, all results related to this type of group can be applied to the additive group within a ring. An ideal in a ring is a special subgroup of the additive group of a ring that is closed under multiplication by ring elements. An ideal is also the kernel of a ring homomorphism. If $R$ is a ring and $a \in R$, we set $(a)$ as the principal ideal generated by $a$. We call a ring where all ideals are principal a principal ideal ring (PIR). Another ideal we are interested in is the Jacobson radical. This ideal is the intersection of all maximal right ideals in the ring. More will be said about the Jacobson radical in the next chapter. A recommended resource for more on rings and ideals is Chapter 12 in [7].

We now introduce some background on results in character theory. The best known resource for more information on character theory is [5]. Character theory is an alternative way to study finite groups and we very briefly point out that ordinary characters of a group are functions into the complex numbers. Throughout this discussion we will always assume the group $G$ is finite. The set $\text{Irr}(G) = \{\theta_1, \ldots, \theta_k\}$ of all irreducible characters of $G$ is the set of characters afforded by irreducible representations. The degree of an irreducible character, $\theta$, is denoted $\theta(1)$. If $\theta = \sum_{i=1}^{k} n_i \theta_i$ is a character, then those $\theta_i$ with $n_i > 0$ are called the irreducible constituents of $\theta$. We mentioned earlier that the number of irreducible characters of a group is equal to the number of conjugacy classes of the group. If $\theta$ is a character of $G$, then $\overline{\theta}$ denotes the complex conjugate.
Let $\varphi$ and $\theta$ be class functions (complex valued functions that remain constant on conjugacy classes) of a group $G$. Then the inner product of $\varphi$ and $\theta$ is defined to be $[\varphi, \theta] = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta(g)}$. If $\varphi$ and $\theta$ are characters, then $[\varphi, \theta] = [\theta, \varphi]$ is a nonnegative integer. Also, $\varphi$ is irreducible if and only if $[\varphi, \varphi] = 1$.

We provide the definition of an induced class function. Let $H \leq G$ and let $\varphi$ be a class function of $H$. Then $\varphi^G$, the induced class function on $G$, is given by

$$\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^o(xgx^{-1}),$$

where $\varphi^o$ is defined by $\varphi^o(h) = \varphi(h)$ if $h \in H$ and $\varphi^o(y) = 0$ if $y \notin H$. An important point to make here is that if $\varphi \in \text{Irr}(H)$, then $\varphi^G$ is a character of $G$, but it is not true in general that $\varphi^G$ is irreducible.

The next lemma is an important tool used quite frequently in character theory and deserves mentioning.

**Lemma 2.21 (Frobenius Reciprocity)** Let $H \leq G$ and suppose that $\varphi$ is a class function on $H$ and that $\theta$ is a class function on $G$. Then $[\varphi, \theta_H] = [\varphi^G, \theta]$, where $\theta_H$ denotes the restriction of $\theta$ to $H$.

A corollary to Frobenius reciprocity states that if $\varphi \in \text{Irr}(H)$, then there exists $\chi \in \text{Irr}(G)$ such that $\varphi$ is a constituent of $\chi_H$.

The main character theory results that we use focus on are those related to normal subgroups. Let $H \triangleleft G$. If $\theta$ is a class function of $H$ and $g \in G$, we define $\theta^g : H \rightarrow \mathbb{C}$ by $\theta^g(h) = \theta(ghg^{-1})$. We say that $\theta^g$ is conjugate to $\theta$. The following is Lemma 6.1 in [5].

**Lemma 2.22** Let $H \triangleleft G$ and let $\varphi, \theta$ be class functions of $H$ and $x, y \in G$. Then
1. \(\varphi^x\) is a class function;

2. \((\varphi^x)^y = \varphi^{xy}\);

3. \([\varphi^x, \theta^x] = [\varphi, \theta]\);

4. \([\chi_H, \varphi^x] = [\chi_H, \varphi]\) for any class function \(\chi\) of \(G\);

5. \(\varphi^x\) is a character if \(\varphi\) is.

We are now ready to introduce what is widely called Clifford theory. The first very important result for our work, which is Theorem 6.2 in [5], is the following.

**Theorem 2.23 (Clifford)** Let \(H \triangleleft G\) and let \(\chi \in \text{Irr}(G)\). Let \(\theta\) be an irreducible constituent of \(\chi_H\) and suppose \(\theta = \theta_1, \theta_2, \ldots, \theta_t\) are the distinct conjugates of \(\theta\) in \(G\). Then \(\chi_H = e \sum_{i=1}^{t} \theta_i\), where \(e = [\chi_H, \theta]\).

The next theorem is arguably the most important tool in character theory. Before we state the theorem we need a definition. Let \(H \triangleleft G\) and let \(\theta \in \text{Irr}(H)\). Then \(I_G(\theta) = \{g \in G|\theta^g = \theta\}\) is called the stabilizer, or inertia group, of \(\theta\) in \(G\). The stabilizer is a subgroup of \(G\) that contains \(H\). From the FCP, \(|G : I_G(\theta)\)| is the size of the orbit of \(\theta\) in the action of \(G\) on the irreducible characters of \(H\). So, from the formula \(\chi_H = e \sum_{i=1}^{t} \theta_i\) in Theorem 2.23, we have that \(t = |G : I_G(\theta)|\).

**Theorem 2.24 (Clifford)** Let \(H \triangleleft G\), \(\theta \in \text{Irr}(H)\), and \(T = I_G(\theta)\). Let

\[
\mathcal{A} = \{\psi \in \text{Irr}(T)|[\psi_H, \theta] \neq 0\} \quad \text{and} \quad \mathcal{B} = \{\chi \in \text{Irr}(G)|[\chi_H, \theta] \neq 0\}.
\]

Then

1. if \(\psi \in \mathcal{A}\), then \(\psi^G\) is irreducible;
2. The map $\psi \mapsto \psi^G$ is a bijection of $A$ onto $B$;

3. If $\psi^G = \chi$, with $\psi \in A$, then $\psi$ is the unique irreducible constituent of $\chi_T$ that lies in $A$;

4. If $\psi^G = \chi$, with $\psi \in A$, then $[\psi_H, \theta] = [\chi_H, \theta]$.

Using the notation of Theorem 2.24, we say that $\theta$ is invariant in $G$ if $T = G$. If $\theta$ is invariant in $G$, then we have $\theta^G = \sum e_i \chi_i$, where $\chi_i \in \text{Irr}(G)$ and $(\chi_i)_H = e_i \theta$. We say that $\theta$ is extendible if $(\chi_j)_H = \theta$ for some $j$. In other words, $e_j = 1$. If $\theta$ is extendible, it is automatically invariant. This leads to the next theorem and a corollary attributed to Gallagher.

**Theorem 2.25** Let $N \triangleleft G$ and let $\varphi, \theta \in \text{Irr}(N)$ be invariant in $G$. Assume $\varphi \theta$ is irreducible and that $\theta$ extends to $\chi \in \text{Irr}(G)$. Let $S = \{\nu \in \text{Irr}(G) | [\varphi^G, \nu] \neq 0\}$ and $T = \{\psi \in \text{Irr}(G) | [\varphi \theta^G, \psi] \neq 0\}$. Then $\nu \mapsto \nu \chi$ defines a bijection of $S$ onto $T$.

Next is Gallagher’s Theorem, which is Theorem 2.25 with $\varphi = 1_N$.

**Corollary 2.26** (Gallagher) Let $N \triangleleft G$ and let $\chi \in \text{Irr}(G)$ be such that $\chi_N = \theta \in \text{Irr}(N)$. Then the characters $\nu \chi$ for $\nu \in \text{Irr}(G/N)$ are irreducible, distinct for distinct $\nu$, and are all of the irreducible constituents of $\theta^G$.

Chapter 6 in [5] is by far the most used resource within this paper, not the least of which are some of the problems at the end of the chapter. We state these as lemmas here, again without proof. In order below are problems 6.1, 6.3, and 6.12 from [5].

**Lemma 2.27** Let $N \triangleleft G$ and $\theta \in \text{Irr}(N)$. Then $\theta^G \in \text{Irr}(G)$ if and only if $I_G(\theta) = N$. 
Problem 6.1, or Lemma 2.27 as it is labeled here, asserts that induced characters of normal subgroups $N$ are irreducible if and only if the stabilizer is only $N$.

Next, problem 6.3 introduces a new type of character known as a fully ramified character. These types of characters are interesting to study and occur throughout [8].

**Lemma 2.28** Let $N \triangleleft G$ and let $\chi \in \text{Irr}(G)$ and $\theta \in \text{Irr}(N)$ with $[\chi_N, \theta] \neq 0$. Then the following are equivalent:

1. $\chi_N = e\theta$, with $e^2 = |G : N|$;
2. $\chi$ vanishes on $G - N$ and $\theta$ is invariant in $G$;
3. $\chi$ is the unique irreducible constituent of $\theta^G$ and $\theta$ is invariant in $G$.

If the hypotheses within Lemma 2.28 are met, we say that $\chi$ and $\theta$ are fully ramified with respect to $G/N$.

The next lemma, problem 6.12, says that a particular character in a particular type of group either induces irreducibly, is fully ramified, or extends. It is sometimes referred to as the ‘going up’ theorem and is directly related to Theorem 6.18 in [5], which is sometimes called the ‘going down’ theorem. We will see later that this result will be relevant to our work, as it was in [9].

**Lemma 2.29** Let $K/L$ be an abelian chief factor of $G$ (i.e., $K, L \triangleleft G$ and no $M \triangleleft G$ exists with $L < M < K$). Let $\varphi \in \text{Irr}(L)$ and $T = I_G(\varphi)$. Assume that $KT = G$. Then one of the following occurs:

1. $\varphi^K \in \text{Irr}(K)$.
2. $\varphi^K = e\theta$ for some $\theta \in \text{Irr}(K)$, where $e^2 = |K : L|$. 
3. \( \varphi^K = \sum_{i=1}^{t} \theta_i \), where \( \theta_i \in \text{Irr}(K) \) are distinct and \( t = |K : L| \).

We feel this chapter provides an ample background for the reader to understand the terminology, notation, and most of the relevant theory used within this paper. As mentioned above, other references provide proofs of the results presented, as well as more detail on the subject matter.
CHAPTER 3

CONSTRUCTION

To begin the construction of our group, we need to place the necessary restrictions on the primes $p$, $q$, and $r$. The $n$th cyclotomic polynomial, denoted $\Phi_n(x)$, is the monic polynomial in $\mathbb{C}[x]$ whose roots are precisely the primitive $n$th roots of unity. Consider the monic polynomial $x^n - 1$. According to Lemma 20.4 in [7], we know that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where the product runs over all positive divisors $d$ of $n$. Notice that $\Phi_1(x) = x - 1$ and, since $x^p - 1 = \Phi_1(x)\Phi_\hat{p}(x)$ for any prime $\hat{p}$, we have $\Phi_\hat{p}(x) = \frac{x^\hat{p}-1}{x-1}$.

We now choose $p$ to be any prime, primes $q < r$, and consider certain cyclotomic polynomials in $p$. Because $q$ and $r$ are primes, we know $\Phi_q(p) = \frac{p^q-1}{p-1}$ and $\Phi_r(p) = \frac{p^r-1}{p-1}$. Since the only divisors of $qr$ are 1, $q, r$, and $qr$, we can write $p^{qr} - 1 = \Phi_1(p)\Phi_q(p)\Phi_r(p)\Phi_{qr}(p)$. Thus, $\frac{p^{qr}-1}{p-1} = \Phi_q(p)\Phi_r(p)\Phi_{qr}(p)$. We choose the distinct primes $q$ and $r$ so that $\Phi_q(p), \Phi_r(p)$, and $\Phi_{qr}(p)$ are pairwise relatively prime.

As was mentioned in Chapter 1, we use the method found in Chapter 4 of [6], as well as in [9], to construct our group $G$. We begin by letting $F$ be the field of order $p^{qr}$ and take $F\{X\}$ to be the skew polynomial ring. A skew polynomial ring gets its name from the slightly unorthodox method of multiplication. In particular, within
the skew polynomial ring the definition of multiplication on the right by a scalars is
given by \( X\alpha = \alpha^p X \) for every element \( \alpha \in F \). A point to make here is that this type
of multiplication is one of the major contributors to complicating the commutator of
elements within our group.

Next we define \( R \) to be the ring obtained from the quotient of \( F\{X\} \) by the ideal
generated by \( X^q+1 \), written \((X^q+1)\). This ideal is the set of all \( \sum_{i\geq q+1} \alpha_i X^i \), where
\( \alpha_i \in F \). Let \( x \) be the image in \( R \) of the indeterminate \( X \). Clearly \( xR = Rx \) is a
nilpotent ideal since \((xR)^q+1 = x^{q+1}R = 0\). Also \( R/xR \cong F \). Hence, \( xR \) is a maximal
ideal of \( R \). In fact, \( xR \) is the unique maximal ideal of \( R \) and therefore, is the Jacobson
radical of \( R \). We will write \( J \) for the Jacobson radical of \( R \). Notice that elements of
\( J \) have the form \( \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_q x^q \) where the \( \alpha_i \in F \).

The Jacobson radical of a ring has some very interesting properties. One such
property is that every element of \( J \) is quasiregular. This means that if \( z \in J \), then
\( 1 - z \) has a multiplicative inverse in \( R \). This is equivalent to the assertion that
\( (1 - z)J = J(1 - z) = J \). A direct consequence of this is that \( 1 + J \) is a subgroup of
the group of units of \( R \). By the fact that \( 1 + J \) is in and of itself then a group, we
know that inverses exist for every element within this structure.

We now define \( P \) to be the group \( 1 + J \). It is clear from the structure of \( J \) that
the elements of \( P \) have the form \( 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_q x^q \) where the \( \alpha_i \in F \). Due
to the size of \( F \) there are \( p^{q^r} \) choices for each of the \( \alpha_i \). Thus, it is easy to see that
the order of \( P \) is \( p^{q^r} \). Also, \( P \) is the unique Sylow \( p \)-subgroup of our group \( G \) that
we are constructing.

As was done in [9], we define \( P^i = 1 + J^i \). Observe that \( P^1 = P \) and \( P^{q+1} = 1 \),
and \( P^i/P^{i+1} \) is isomorphic to the additive group of \( F \) for \( i = 1, 2, \ldots q \). It is easy to
see that \( P^i \) is normal in \( G \) for every positive integer \( i \). Another important note is that
$P^{\frac{q-1}{2}}$ is abelian and $P^k$ is not abelian for $k = 1, 2, \ldots, \frac{q-1}{2}$. This family of $p$-groups has within it quotient groups that behave in such a manner that we can apply results from [16] to factor groups within this family, as we will see later.

We now introduce some group actions. Since $F^\times$ is cyclic of order divisible by $p - 1$, we know from Theorem 2.9 of [7] that there is a unique subgroup $C$ of $F^\times$ of order $\frac{p^q - 1}{p - 1}$. There is a natural action of $C$ on $R$ via automorphisms defined by $\left(\sum_{i=1}^{q} \alpha_i x^i\right) \star c = \sum_{i=1}^{q} \alpha_i c^{p^i} x^i$. However, we define a different action on $R$.

Consider the subgroup $F_0^\times$ of $F^\times$ of order $p - 1$. From Lemma 4.6 in [6], we know that $F^\times = C \times F_0^\times$. This fact plays a crucial role in determining the action of $C$ on $R$. As in [9], we define the action of $C$ on $R$ via ring automorphisms by

$$(\alpha_0 + \alpha_1 x + \cdots + \alpha_q x^q) \cdot c = \alpha_0 c^0 + \alpha_1 c^p x + \cdots + \alpha_q c^{p^{q-1}} x^q.$$  

To see that this is a group action, first notice that if $t = \alpha_0 + \alpha_1 x + \cdots + \alpha_q x^q$, then $t \cdot 1 = t$. Also, if $c, d \in C$, then

$$(t \cdot c) \cdot d = (\alpha_0 + \alpha_1 c^{p^{q-1}} x + \cdots + \alpha_q c^{p^{q-1}} x^q) \cdot d$$

$$= \alpha_0 + \alpha_1 c^{p^{q-1}} d^{p^{q-1}} x + \cdots + \alpha_q c^{p^{q-1}} d^{p^{q-1}} x^q$$

$$= \alpha_0 + \alpha_1 (cd)^{p^{q-1}} x + \cdots + \alpha_q (cd)^{p^{q-1}} x^q = t \cdot (cd).$$

To see that $C$ acts via ring automorphisms, let $r_1 = \alpha_0 + \alpha_1 x + \cdots + \alpha_q x^q, r_2 = \beta_0 + \beta_1 x + \cdots + \beta_q x^q \in R$, and $c \in C$. Then

$$(r_1 + r_2) \cdot c = ((\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) x + \cdots + (\alpha_q + \beta_q) x^q) \cdot c.$$
Using the definition of the action, we extend this to

\[(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)cx + \cdots + (\alpha_q + \beta_q)c^{\frac{q-1}{p-1}}x^q = (\alpha_0 + \beta_0) + \cdots + (\alpha_q c^{\frac{q-1}{p-1}} + \beta_q c^{\frac{q-1}{p-1}})x^q.\]

Distributing \(x^i\) within each term and combining like terms we obtain

\[(\alpha_0 + \alpha_1 cx + \cdots + \alpha_q c^{\frac{q-1}{p-1}}x^q) + (\beta_0 + \beta_1 cx + \cdots + \beta_q c^{\frac{q-1}{p-1}}x^q) = (r_1 \cdot c) + (r_2 \cdot c).\]

Now that we know the action of \(C\) on \(R\) preserves ring addition, we can verify the preservation of products using monomials as representative elements of \(R\). Let \(r_1 = \alpha_i x^i, r_2 = \alpha_j x^j \in R, c \in C,\) and assume \(i + j \leq q\). Then \((r_1 r_2) \cdot c = (\alpha_i \alpha_j^{p^i} x^{i+j}) \cdot c.\)

The definition of the action gives the expression

\[\alpha_i \alpha_j^{p^i} c^{\frac{p^{i+j}-1}{p-1}} x^{i+j}. \quad (3.1)\]

We now consider

\[(r_1 \cdot c)(r_2 \cdot c) = \alpha_i c^{\frac{p^i-1}{p-1}}x^i \alpha_j c^{\frac{p^j-1}{p-1}}x^j.\]

Multiplication within the skew polynomial ring and combining exponents of \(c\) gives us

\[\alpha_i \alpha_j^{p^i} c^{\frac{p^{i+j}-1}{p-1}}x^{i+j} = \alpha_i \alpha_j^{p^i} c^{\frac{p^i-1}{p-1}} r_1 \cdot c^{\frac{p^{i+j}-1}{p-1}}x^{i+j}.\]

Lastly, by simplifying the exponent of \(c\) we have the expression

\[\alpha_i \alpha_j^{p^i} c^{\frac{p^{i+j}-1}{p-1}} x^{i+j},\]

which equals (3.1). Hence, \(C\) acts via ring automorphisms on \(R\).

Let \(G\) be the Galois group of \(F\) over the subfield of order \(p\). Theorem 2.17 tells
us that \( G \) is cyclic of order \( qr \). For any element \( \sigma \in G \) we define the action of \( G \) on \( R \) to be

\[
(\alpha_0 + \alpha_1 x + \cdots + \alpha_q x^q) \cdot \sigma = \alpha_0^\sigma + \alpha_1^\sigma x + \cdots + \alpha_q^\sigma x^q,
\]

where the \( \alpha_i \in F \), and the action of \( \sigma \) on \( C \) is just the action of \( \sigma \) on \( F^x \). It is not difficult to see that \( G \) acts via automorphisms on \( R \). Let \( \sigma \in G \) and set \( r_1 = \alpha_0 + \alpha_1 x + \cdots + \alpha_q x^q \) and \( r_2 = \beta_0 + \beta_1 x + \cdots + \beta_q x^q \). Then

\[
(r_1 + r_2) \cdot \sigma = ((\alpha_0 + \cdots + \alpha_q x^q + \beta_0 + \cdots + \beta_q x^q)) \cdot \sigma = ((\alpha_0 + \beta_0) + \cdots + (\alpha_q + \beta_q) x^q) \cdot \sigma.
\]

The definition of the Galois action and the fact that \( \sigma \) is a subgroup of \( Aut(F) \) gives us

\[
(\alpha_0 + \beta_0)^\sigma + \cdots + (\alpha_q + \beta_q)^\sigma x^q = (\alpha_0^\sigma + \beta_0^\sigma) + \cdots + (\alpha_q^\sigma + \beta_q^\sigma) x^q.
\]

By distributing each \( x^i \) and combining like terms, we have

\[
(\alpha_0^\sigma + \cdots + \alpha_q^\sigma x^q) + (\beta_0^\sigma + \cdots + \beta_q^\sigma x^q) = (r_1 \cdot \sigma) + (r_2 \cdot \sigma).
\]

Again, to show the action of \( G \) on \( R \) preserves ring multiplication, we can use monomials as representative elements of \( R \). Let \( \sigma \in G \), and \( r_1 = \alpha_i x^i, r_2 = \beta_j x^j \in R \). Then

\[
(r_1 r_2) \cdot \sigma = (\alpha_i x^i \beta_j x^j) \cdot \sigma = (\alpha_i \beta_j^p x^{i+j}) \cdot \sigma.
\]

Using the definition of the action and that \( \sigma \) is an automorphism of \( F \), we have

\[
(\alpha_i \beta_j^p)^\sigma x^{i+j} = \alpha_i^\sigma (\beta_j^p)^\sigma x^{i+j} = \alpha_i^\sigma (\beta_j^p)^{i+j}.
\]
Reassociating this product yields

\[(\alpha_i^\sigma x^i)(\beta_j^\sigma x^j) = (r_1 \cdot \sigma)(r_2 \cdot \sigma).\]

Therefore, \(G\) acts via ring automorphisms on \(R\). Clearly, \(G\) also acts on \(C\) via automorphisms. Hence, we form the semidirect product of \(G\) with \(C\). Suppose \(\alpha_ix^i \in R, c \in C,\) and \(\sigma \in G\). To show that \(GC\) acts via automorphisms on \(R\), we need to show \((\alpha_ix^i) \cdot c \cdot \sigma = ((\alpha_ix^i) \cdot \sigma) \cdot c^\sigma\). We begin by noticing from the left side of the equation

\[((\alpha_i x^i) \cdot c) \cdot \sigma = (\alpha_i c^{\frac{p-1}{\rho-1}} x^i) \cdot \sigma = \alpha_i^\sigma (c^{\frac{p-1}{\rho-1}})^\sigma x^i.\]

Again, \(\sigma\) is an automorphism. So, the right hand side becomes \(\alpha_i^\sigma (c^{\frac{p-1}{\rho-1}} x^i\). Separating this product gives us

\[(\alpha_i^\sigma x^i) \cdot c^\sigma = ((\alpha_i x^i) \cdot \sigma) \cdot c^\sigma.\]

Therefore, \(GC\) acts on \(R\) via automorphisms. Notice \(P\) is invariant under this action. We now construct our group \(G\) from the semidirect product of \(GC\) with \(P\).

For the appropriate fixed primes, the order of the group is very large. The order of \(G\) is \(qrpq^{\sigma+\mu}(\frac{p-1}{p-1})\). Even in the case presented by Lewis, his group had order in the neighborhood of \(10^{19}\). Whether or not a smaller example of a solvable group with a degree graph of diameter three exists is not known, as of yet.
CHAPTER 4

BILINEAR FORMS

The results in this chapter do not involve the characters of our group directly but will play an important role in helping us understand the kernels of our characters better. Also, many complicated strings of sums occur later when we look at commutators of elements inside of $P$. The lemmas here eliminate some of the work later.

Throughout this chapter, unless otherwise noted, we will let $F = GF(p^f)$, where $p$ is any prime and let $m, n \in \mathbb{Z}^+$. In keeping with methods used in [9], we generalize the definition of maps used in that paper to characterize the coefficients in $P$ that occur.

We begin by defining the map $\langle \cdot, \cdot \rangle_{m,n}$ from $F \times F \rightarrow F$ by

$$\langle a, b \rangle_{m,n} = ab^{p^m} - a^{p^n}b.$$ 

We define $\langle a, F \rangle_{m,n} = \{ \langle a, b \rangle_{m,n} \mid b \in F \}$. Note that if $a = 0$, then $\langle a, F \rangle_{m,n} = \{0\}$. This map has several useful and interesting properties. Those properties that are needed for the purposes of this paper are outlined in this chapter. In general, as we will see below, the nature of these forms will depend on $gcd(m,n)$, $gcd(m,f)$, and $gcd(m+n,f)$. 

27
Lemma 4.1 Let $d = \gcd(m, n)$ and suppose $d \mid f$. Let $F_d$ be the subfield of $F$ of order $p^d$. Then the map $\langle \cdot, \cdot \rangle_{m,n}$ from $F \times F \to F$ defined by $\langle a, b \rangle_{m,n} = ab^{p^m} - a^p b$ is an $F_d$-bilinear map. In particular, if we fix $a \in F$, the map $\langle a, \cdot \rangle_{m,n} : F \to F$ is an additive homomorphism.

Proof. Let $\alpha, \beta \in F_d$ and $a_1, a_2, b \in F$. To show linearity in the first coordinate of $\langle \cdot, \cdot \rangle_{m,n}$ we will need to show that

$$
\langle \alpha a_1 + \beta a_2, b \rangle_{m,n} = \alpha \langle a_1, b \rangle_{m,n} + \beta \langle a_2, b \rangle_{m,n}.
$$

By definition of $\langle \cdot, \cdot \rangle_{m,n}$, we see that

$$
\langle \alpha a_1 + \beta a_2, b \rangle_{m,n} = (\alpha a_1 + \beta a_2)^{p^m} - (\alpha a_1 + \beta a_2)^{p^n} b.
$$

Since the characteristic of $F$ is $p$, we have that for all $\gamma$ and $\delta$ in $F$, $(\gamma \pm \delta)^{p^k} = \gamma^{p^k} \pm \delta^{p^k}$ for any integer $k$. We use this fact to expand the last expression and get

$$
(\alpha a_1 + \beta a_2)^{p^m} - (\alpha a_1 + \beta a_2)^{p^n} b = \alpha a_1 b^{p^m} + \beta a_2 b^{p^m} - (\alpha a_1)^{p^m} b - (\beta a_2)^{p^n} b
$$

$$
= \alpha a_1 b^{p^m} - \alpha^{p^n} a_1^{p^n} b + \beta a_2 b^{p^m} - \beta^{p^n} a_2^{p^n} b.
$$

Now, $o(\alpha)$ and $o(\beta)$ both divide $p^d - 1$ since $\alpha$ and $\beta$ are elements of $F_d$. As a result $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. Hence,

$$
\alpha a_1 b^{p^m} - (\alpha a_1)^{p^n} b + \beta a_2 b^{p^m} - (\beta a_2)^{p^n} b = \alpha a_1 b^{p^m} - \alpha a_1^{p^n} b + \beta a_2 b^{p^m} - \beta a_2^{p^n} b.
$$
And again by definition of $\langle \cdot, \cdot \rangle_{m,n}$, we have

$$aa_1b^{p^m} - aa_1^{p^n}b + \beta a_2b^{p^m} - \beta a_2^{p^n}b = \alpha(aa_1b^{p^m} - a_1^{p^n}b) + \beta(a_2b^{p^m} - a_2^{p^n}b)$$

$$= \alpha\langle a_1, b \rangle_{m,n} + \beta\langle a_2, b \rangle_{m,n}.$$ 

Linearity in the second coordinate can be shown using a similar argument. The last statement of the lemma follows immediately from $\langle \cdot, \cdot \rangle_{m,n}$ being $F_d$-bilinear. \(q.e.d.\)

We should mention some easy, yet relevant, facts regarding $\langle a, b \rangle_{m,n}$. First, notice that

$$\langle a, b \rangle_{m,n} = ab^{p^m} - a^{p^n}b = -(a^{p^n}b - ab^{p^m}) = -\langle b, a \rangle_{n,m}.$$ 

This result will be used frequently without mention. Secondly, this clearly implies the fact that $\langle a, F \rangle_{m,n} = \langle F, a \rangle_{n,m}$. Formal proofs of these results are omitted.

The importance of calculating stabilizers of the various characters is to help compute character degrees by applying well-known Clifford theory. The first few results in this chapter help us get a handle on the behavior that the commutators exhibit.

Of equal importance are the kernels of our characters. Later results in this chapter will be used to help us describe the kernels of certain characters. The next two lemmas will be used directly and quite frequently when computing coefficients of the various powers of $x$ within the commutators.

**Lemma 4.2** Let $a, b \in F$. Then $a(\langle a, b \rangle_{m,n})^{p^m} = \langle a, ab^{p^m} \rangle_{m,m+n}.$

**Proof.** By definition of $\langle \cdot, \cdot \rangle_{m,n}$ we have that

$$a(\langle a, b \rangle_{m,n})^{p^m} = a(ab^{p^m} - a^{p^n}b)^{p^m}.$$
Recall from the proof of Lemma 4.1 that since the characteristic of $F$ is $p$, we know that for any $\alpha$ and $\beta$ in $F$, $(\alpha - \beta)^p = \alpha^p - \beta^p$. Hence,

$$a(ab^m - a^p b)^p = a((ab^m)^p - a^{p^m + b^p}).$$

By distributing $a$, we have

$$a[(ab^m)^p - a^{p^m + b^p}] = a(ab^m)^p - a^{p^m + n}(ab^m).$$

And finally, by definition of $\langle \cdot, \cdot \rangle_{m,n}$ we have

$$a(ab^m)^p - a^{p^m + n}(ab^m) = \langle a, ab^m \rangle_{m,m+n}.$$ 

q.e.d.

Continuing on the same topic, this next lemma will handle a slightly more complicated calculation that appears later. This lemma helps us pair two separate forms together that have the appropriate parameters. Notice the similarities and differences between Lemma 4.2 and this next lemma.

**Lemma 4.3** Let $a, b, c \in F$. Then

$$a((b, c)_{m,n})^{pk} + b((a, c)_{k,n})^{pn} = \langle a, bc^p \rangle_{k,m+n} + \langle b, ac^k \rangle_{m,k+n}.$$ 

**Proof.** We begin as usual and notice that

$$a((b, c)_{m,n})^{pk} + b((a, c)_{k,n})^{pn} = a(bc^p - b^p c)^p + b(ac^k - a^p c)^p.$$
Recall that $F$ has characteristic $p$, so

$$a[(bc^p^n - b^p^n c)^p^k] + b[(ac^p^n - a^p^n c)^p^m]$$

$$= a[(bc^p^m)^p^k - (b^p^n c)^p^k] + b[(ac^p^n)^p^m - (a^p^n c)^p^m].$$

Expanding this further we have

$$a[(bc^p^m)^p^k - (b^p^n c)^p^k] + b[(ac^p^n)^p^m - (a^p^n c)^p^m]$$

$$= ab^p^k c^{p^k + m} - ab^p^{k+n} c^p^k + ba^p^n c^{p^k + m} - ba^p^{m+n} c^p^m.$$ 

If we group the first term from this with the fourth term and the second term with the third, we obtain

$$ab^p^k c^{p^k + m} - ab^p^{k+n} c^p^k + ba^p^n c^{p^k + m} - ba^p^{m+n} c^p^m$$

$$= ab^p^k c^{p^k + m} - ba^p^{m+n} c^p^m + ba^p^n c^{p^k + m} - ab^p^{k+n} c^p^k.$$ 

The result now follows since, by definition,

$$ab^p^k c^{p^k + m} - ba^p^{m+n} c^p^m + ba^p^n c^{p^k + m} - ab^p^{k+n} c^p^k$$

$$= \langle a, bc^p^m \rangle_{k,m+n} + \langle b, ac^p^n \rangle_{m,k+n}.$$ 

q.e.d.

We now move on to information regarding the general maps. In the next few lemmas we determine much needed information regarding the kernels of these maps. We also compare the kernels of these maps to the kernel of the trace map. As we will
see, there is a direct relationship between the kernels of these maps and the kernel of the trace map when \( \gcd(m, f) = 1 \).

**Lemma 4.4** Suppose \( d = \gcd(m, f) \) and let \( 0 \neq a \in F \). Assume \( \gcd(p^m - 1, \frac{p^f - 1}{p^d - 1}) = 1 \). Define the map \( a_{m,n} : F \rightarrow F \) by \( a_{m,n}(b) = \langle a, b \rangle_{m,n} \) for all \( b \in F \). If \( o(a^{p^n - 1}) \) does not divide \( \frac{p^f - 1}{p^d - 1} \), then \( \ker(a_{m,n}) = 0 \) and \( \langle a, F \rangle_{m,n} = F \). Otherwise, \( \vert \ker(a_{m,n}) \vert = p^d \) and \( \vert \langle a, F \rangle_{m,n} \vert = p^{f-d} \).

**Proof.** Note that \( a_{m,n} \) is an additive homomorphism and that

\[
\text{Im}(a_{m,n}) = \langle a, F \rangle_{m,n} \subseteq F.
\]

By the First Isomorphism Theorem, we know that

\[
\vert \langle a, F \rangle_{m,n} \vert = \frac{\vert F \vert}{\vert \ker(a_{m,n}) \vert}.
\]

So we work to compute \( \vert \ker(a_{m,n}) \vert \).

Suppose \( b \in \ker(a_{m,n}) \). Now, \( 0 \in \ker(a_{m,n}) \), so without loss we can assume \( b \neq 0 \).

Thus, \( 0 = \langle a, b \rangle_{m,n} = ab^{p^m} - ba^{p^n} \). Since \( a \) and \( b \) are not zero, this implies that \( b^{p^m - 1} = a^{p^n - 1} \).

Since \( d \mid m \), we can write \( p^m - 1 = (p^d - 1)h(p) \) for some polynomial \( h \). Notice that

\[
\left( b^{p^m - 1} \right)^{\frac{p^f - 1}{p^d - 1}} = (b^{h(p)})^{p^f - 1} = 1.
\]

So, \( o(b^{p^m - 1}) \mid \frac{p^f - 1}{p^d - 1} \). Since we know that \( o(b^{p^m - 1}) = o(a^{p^n - 1}) \), if \( o(a^{p^n - 1}) \) does not divide \( \frac{p^f - 1}{p^d - 1} \), this is a contradiction, and we conclude that \( \ker(a_{m,n}) = \{0\} \). Hence, \( \vert \langle a, F \rangle_{m,n} \vert = \vert F \vert \) and so \( F = \langle a, F \rangle_{m,n} \).

Now assume \( o(a^{p^n - 1}) \mid \frac{p^f - 1}{p^d - 1} \). Our field \( F \) is finite and therefore \( F^\times \) is cyclic by Lemma 17.12 in [5]. According to Theorem 2.9 in [5], for each divisor of \( p^f - 1 \), there is exactly one subgroup of \( F^\times \). In particular, \( F^\times \) has a unique subgroup, \( B^\times \),
of order $\frac{p^d-1}{p^d-1}$. Since $gcd(p^m - 1, \frac{p^d-1}{p^d-1}) = 1$, raising the elements of $B^\times$ to the power $p^m - 1$ induces a bijection on $B^\times$, so there exists a unique element $b_0 \in B^\times$ such that $b_0^{p^m-1} = a^{p^n-1}$. Since $\frac{p^d-1}{p^d-1}$ and $p^d - 1$ are relatively prime, we can write $b = b_0c$ for $c \in GF(p^d)$ where $b_0^{p^m-1} = a^{p^n-1}$. Hence, $b^{p^m-1} = b_0^{p^m-1}c^{p^m-1}$.

Recall that we can write $p^m - 1 = (p^d - 1)h(p)$ for some polynomial $h$. So, $b_0^{p^m-1}c^{p^m-1} = b_0^{p^m-1}c^{(p^d-1)(h(p))}$. Our choices of $b_0$ and $c$ yield $b_0^{p^m-1}c^{(p^d-1)(h(p))} = a^{p^n-1}$. But this forces $b^{p^m-1} = a^{p^n-1}$, which is true if $b \in \ker(a_{m,n})$. Thus, the elements of $\ker(a_{m,n})$ are in one to one correspondence with the elements of $GF(p^d)$. Therefore, $|\ker(a_{m,n})| = p^d$ and via the First Isomorphism Theorem, $|\langle a, F \rangle_{m,n}| = p^{f-d}$. q.e.d.

Before we begin the next few lemmas, we take a moment to mention our definition and a few of the properties of trace maps. Our definition is actually taken from Theorem 23.5 in [5].

Suppose $E$ is a finite field extension of $K$ and suppose $\alpha$ is an element of $E$. Let $m = |E : K[\alpha]|$. Finally, let $s$ denote the sum of the roots of the minimal polynomial of $\alpha$ over $K$, counting multiplicities. We define $Tr_{E/K}(\alpha) = ms$.

We also mention two corollaries from [5], 23.10 and 23.11, that have relevance to our purposes here. Let $L \leq K \leq E$, where $E$ is Galois over $L$, and let $U$ be a set of representatives for the right cosets of $Gal(E/K)$ in $Gal(E/L)$. Then $Tr_{K/L}(\alpha) = \sum_{\sigma \in U} \alpha^\sigma$ for all $\alpha \in K$. The second corollary is a special case of Corollary 23.10 where $K$ is Galois over $L$. Here we can take $E = K$. The corollary states that if we let $L \leq K$ be Galois with $G = Gal(K/L)$, then $Tr_{K/L}(\alpha) = \sum_{\sigma \in G} \alpha^\sigma$ for all $\alpha \in K$.

One important property of the trace map is the $L$-linearity of the map. In other words, for elements $\alpha, \beta \in K$ and scalars $a, b \in L$, we have $Tr_{K/L}(a\alpha + b\beta) = aTr_{K/L}(\alpha) + bTr_{K/L}(\beta)$. If the characteristic of $L$ is $p$ and $L = GF(p)$, then
\[ Tr_{K/L}(\alpha^p) = Tr_{K/L}(\alpha) \] for all \( \alpha \in K \). Unless otherwise stated, we will use the notation \( Tr \) to denote the trace \( Tr_{F/GF(p)} : F \rightarrow GF(p) \).

A subspace \( K \), of a vector space \( E \) over \( GF(p) \), is called a hyperplane for \( E \) if it has dimension one less than \( E \). From Lemma 4.4, we saw that \( | \langle a, F \rangle_{m,n} | = p^{f-d} \). Thus, the subspace \( \langle a, F \rangle_{m,n} \) is a hyperplane in \( F \) if and only if \( d = 1 \). Notice that the First Isomorphism Theorem tells us that \( | \ker(Tr) | = p^{f-1} \), hence \( \ker(Tr) \) will also be a hyperplane. The hyperplanes within our group correspond to the kernel of the trace map. This correspondence may, or may not be one-to-one, as we will see below.

**Lemma 4.5** Let \( d = \gcd(m + n, f) \). If \( a \in GF(p^d) \), then \( \langle a, F \rangle_{m,n} \subseteq \ker(Tr) \). In particular, \( \langle a, F \rangle_{m,n} = \ker(Tr) \) if and only if \( \gcd(m, f) = 1 \).

**Proof.** Let \( a \in GF(p^d) \) and \( b \in F \). Using the definition of \( \langle \cdot, \cdot \rangle_{m,n} \) and the linearity of the trace map, we have

\[
Tr(\langle a, b \rangle_{m,n}) = Tr(ab^{p^m} - a^{p^n}b) = Tr(ab^{p^m}) - Tr(a^{p^n}b).
\]

The property that \( Tr(\alpha^p) = Tr(\alpha) \) for all \( \alpha \in F \) gives us

\[
Tr(ab^{p^m}) - Tr(a^{p^n}b) = Tr(ab^{p^m}) - Tr((a^{p^n}b)^{p^m}) = Tr(ab^{p^m}) - Tr(a^{p^{m+n}}b^{p^m}).
\]

By linearity we obtain

\[
Tr(ab^{p^m}) - Tr(a^{p^{m+n}}b^{p^m}) = Tr(ab^{p^m} - a^{p^{m+n}}b^{p^m}) = Tr((a - a^{p^{m+n}})b^{p^m}).
\]
Since by assumption $d \mid m + n$ and $a \in GF(p^d)$, we have that $a^{p^{n+m}} = a$, and so,
\[ Tr((a - a^{p^{n+m}})b^m) = Tr((a - a)b^m) = 0. \]

Hence, $\langle a, F \rangle_{m,n} \subseteq \ker(Tr)$.

As discussed above, $\langle a, F \rangle_{m,n} = \ker(Tr)$ if and only if $\langle a, F \rangle_{m,n}$ is a hyperplane in $F$. Thus, $\langle a, F \rangle_{m,n} = \ker(Tr)$ if and only if $\gcd(m, f) = 1$.

**Corollary 4.6** In general we have $\langle 1, F \rangle_{m,n} \subseteq \ker(Tr)$. In particular, $\langle 1, F \rangle_{m,n} = \ker(Tr)$ if and only if $\gcd(m, f) = 1$.

This is an immediate consequence of Lemma 4.5 with $a = 1$.

**Lemma 4.7** Let $d = \gcd(m, f)$. Assume $\gcd(p^d - 1, \frac{f}{d}) = 1$. Write $a = a_0 c$ where $o(a_0) \mid (p^d - 1)$ and $o(c) \mid \left(\frac{p(f-1)}{p-1}\right)$. Then $\langle a, F \rangle_{m,n} \subseteq c^{(p^{n+m} - 1)k} \langle a_0, F \rangle_{m,n}$ where $k \equiv (p^n - 1)^{-1} \mod\left(\frac{p^d - 1}{p-1}\right)$. In particular, $\langle a, F \rangle_{m,n} = c^{(p^{n+m} - 1)k} \ker(Tr)$ if and only if $\gcd(m, f) = 1$ and $o(a^{p-1}) \mid \left(\frac{p(f-1)}{p-1}\right)$.

**Proof.** Let $b \in F$. Since $F$ is a field, we can write $b = b_0 c^{(p^n - 1)k}$ for some $b_0 \in F$.

Then substituting appropriately for $a$ and $b$ and by definition of $\langle \cdot, \cdot \rangle_{m,n}$, we have
\[ \langle a, b \rangle_{m,n} = \langle a_0 c, b_0 c^{(p^n - 1)k} \rangle_{m,n} = (a_0 c)(b_0 c^{(p^n - 1)k})^{p^m} - (a_0 c)^p (b_0 c^{(p^n - 1)k}). \]

From here we see that
\[ (a_0 c)(b_0 c^{(p^n - 1)k})^{p^m} - (a_0 c)^p (b_0 c^{(p^n - 1)k}) = a_0 c b_0^{p^m} c^{p^m (p^n - 1)k} - a_0^p c^{p^m} b_0 c^{(p^n - 1)k}. \]
By combining the exponents of \(c\) in each term, we are left with

\[
a_0c_b^m c^{p^m(p^n-1)k} - a_0^n c^p b_0 c^{(p^n-1)k} = c^{1+p^m(p^n-1)k} a_0 b^m - c^{p^m(p^n-1)k} a_0^n b_0.
\]

We now compare the exponents of \(c\) in each term in the last expression. We begin with the exponent of \(c\) in the first term. Recalling that the choice of \(k\) gives \(1 \equiv k(p^m-1)\), we have \(1+p^m(p^n-1)k = 1+kp^{m+n}-kp^m \equiv k(p^m-1)+k(p^{m+n}-p^m) = k(p^m-1+k(p^{m+n}-p^m)) = k(p^{m+n}-1).\) Similarly, working with the exponent of \(c\) in the second term, we have \(p^n+kp^n-k \equiv k(p^m-1)p^n + kp^n - k = k(p^{m+n} - p^n + p^n - 1) = k(p^{m+n} - 1).\) Now, we have

\[
c^{1+p^m(p^n-1)k} a_0 b^m - c^{p^m(p^n-1)k} a_0^n b_0 = c^k(p^{m+n}-1)(a_0 b^m - a_0^n b_0).
\]

Again, by definition of \(\langle \cdot, \cdot \rangle_{m,n}\) we have

\[
c^k(p^{m+n}-1)(a_0 b^m - a_0^n b_0) = c^{k(p^{m+n}-1)}(a_0, b_0)_{m,n}.
\]

Therefore, \(\langle a, F \rangle_{m,n} \subseteq c^{(p^{m+n}-1)k} \langle a_0, F \rangle_{m,n}\) and the first part of the lemma is proven.

Suppose \(\langle a, F \rangle_{m,n} = c^{(p^{m+n}-1)k} \ker(Tr).\) Thus, \(| \langle a, F \rangle_{m,n} | = | \ker(Tr) | = p^{f-1}.\) By Lemma 4.4, we have \(o(a^{p^n}) | p^{f-1} \) and \(gcd(m, f) = 1.\) Conversely, suppose \(o(a^{p^n})\) divides \(\frac{p^{f-1}}{p^r-1}\) and \(gcd(m, f) = 1.\) Then by Lemma 4.4, \(| \langle a, F \rangle_{m,n} | = p^{f-1}.\) By Lemma 4.5, \(\langle a_0, F \rangle_{m,n} = \ker(Tr),\) so \(\langle a, F \rangle_{m,n} \subseteq c^{(p^{m+n}-1)k} \ker(Tr).\) Since \(| \langle a, F \rangle_{m,n} | = p^{f-1} = | \ker(Tr) | ,\) we see that equality follows.

\[q.e.d.\]

**Corollary 4.8** Let \(f = qr\) where \(q < r\) are primes. If \(0 < i < q\) and \(\alpha \in F,\) then \(\langle \alpha, F \rangle_{i,q-i} = c^{(p^i-1)k} \ker(Tr)\) for some element \(c \in F\) so that \(o(c)\) divides \(\frac{p^{f-1}}{p^r-1}.\)
Furthermore, for each such $c$, there is an $\alpha$ so that $\langle \alpha, F \rangle_{i,q} = c^{(p^q - 1)k} \ker(Tr)$. Therefore, the set of hyperplanes of the form $\langle \alpha, F \rangle_{i,q} - i$ is the set of hyperplanes $c^{(p^q - 1)k} \ker(Tr)$ as $c$ runs through the elements of $F$ of order $\frac{p^f - 1}{p^r - 1}$. In particular, this second set of hyperplanes is independent of $i$.

**Proof.** In the situation of Lemma 4.7, we can let $d = q$, $m = i$, and $n = q - i$. We then have $\langle \alpha, F \rangle_{i,q} = c^{(p^q - 1)k} \ker(Tr)$, where $o(c) \mid \frac{p^f - 1}{p^r - 1}$ and $k \equiv (p^i - 1)^{-1} \mod(\frac{p^f - 1}{p^r - 1})$. As in Lemma 4.7, for each such $c$ we can write $\alpha = \alpha_0 c$ where $o(\alpha_0) \mid p^q - 1$. As a result, the set of hyperplanes of the form $\langle \alpha, F \rangle_{i,q} - i$ is the set of hyperplanes $c^{(p^q - 1)k} \ker(Tr)$ as $c$ runs through the elements of $F$ of order $\frac{p^f - 1}{p^r - 1}$, and this set is independent of $i$. q.e.d.

The following two lemmas are special cases of Lemma 4.7 where in each case $m$ and $f$ are relatively prime. The purpose of these lemmas will become clear in the last chapter of this paper.

**Lemma 4.9** Let $a \in F$ such that $o(a) \mid \frac{p^f - 1}{p - 1}$. Choose $c \in \mathbb{Z}^+$ so that

$$c \equiv (p^m - 1)^{-1} \mod(o(a)).$$

Set $b \equiv c(p^m - 1) \mod(o(a))$. Then $\langle a, F \rangle_{m,n} = \langle F, a^b \rangle_{m,n}$.

**Proof.** By Lemma 4.7 we know that $\langle a, F \rangle_{m,n} = a^{\frac{p^m n + 1}{p^m - 1}} \ker(Tr)$. On the other hand, we also know from Lemma 4.7 that $\langle F, a^b \rangle_{m,n} = \langle a^b, F \rangle_{n,m} = a^{b\left(\frac{p^m n + 1}{p^m - 1}\right)} \ker(Tr)$. Our choice of $b$ gives the desired result since

$$b \left(\frac{p^{m+n} - 1}{p^n - 1}\right) \equiv \left(\frac{p^n - 1}{p^m - 1}\right) \left(\frac{p^{m+n} - 1}{p^n - 1}\right) = \frac{p^{m+n} - 1}{p^m - 1}.$$  

q.e.d.
Lemma 4.10 Let \( a \in F \) such that \( o(a) \mid \frac{q^r - 1}{p-1} \). Choose \( b \in \mathbb{Z}^+ \) such that \( b \equiv (\frac{q^r - 1}{p-1}) \mod(o(a)) \). Then \( \langle a, F \rangle_{1,m-1} = \langle a^b, F \rangle_{n,m-n} \).

**Proof.** As in the proof of Lemma 4.9, we know from Lemma 4.7 that \( \langle a, F \rangle_{1,m-1} = a^{\frac{p^m - 1}{p-1}} \ker(Tr) \). Similarly, we have that \( \langle a^b, F \rangle_{n,m-n} = a^{b(\frac{p^m - 1}{p-1})} \ker(Tr) \). The given choice of \( b \) yields

\[
\frac{b(p^m - 1)}{p^m - 1} \equiv \frac{(p^m - 1)}{p - 1} \left( \frac{p^m - 1}{p^n - 1} \right) = \frac{p^m - 1}{p - 1}.
\]

q.e.d.

The last two lemmas of this chapter characterize all of the hyperplanes in our field \( F \). For these two lemmas we assume we are within our group \( G \).

Lemma 4.11 Assume \( a \in F \) and \( a \neq 0 \). Then \( a \ker(Tr) = \ker(Tr) \) if and only if \( a \in \mathbb{Z}_p \).

**Proof.** If \( a \in \mathbb{Z}_p \), then \( a \ker(Tr) = \ker(Tr) \) since multiplication by elements in \( \mathbb{Z}_p \) does not affect whether or not the trace is zero.

Conversely, suppose \( a \ker(Tr) = \ker(Tr) \) and assume \( a \notin \mathbb{Z}_p \). Thus, \( a - a^p \neq 0 \). Let \( d \in F \) with \( Tr(d) \neq 0 \). Let \( c \in F \) so that \( (a - a^p)c = d \). Since multiplication by elements in \( \mathbb{Z}_p \) does affect whether or not the trace is zero, we may assume \( o(c) \) divides \( \frac{p^r - 1}{p-1} \). Because \( a \ker(Tr) = \ker(Tr) \), it follows that \( a(\gamma - \gamma^p) \in \ker(Tr) \) for all \( \gamma \in F \).

By the definition of the kernel of the trace map, we know that \( a\gamma - (a\gamma)^p \in \ker(Tr) \). Subtracting these terms, we have \( a\gamma^p - a^p\gamma^p - (a - a^p)\gamma^p \in ker Tr \) for all \( \gamma \in F \). Now, raising to the \( p \)-power is a bijection for the cyclic group of order \( \frac{p^r - 1}{p-1} \), so there is a \( \gamma \in F \) so that \( \gamma^p = c \). This yields \( (a - a^p)\gamma^p = (a - a^p)c = d \notin \ker(Tr) \). This is a contradiction. Therefore, \( a \in \mathbb{Z}_p \). q.e.d.
Lemma 4.12 Every hyperplane in $F$ has the form $a \ker(Tr)$ for some $0 \neq a \in F$.

Proof. Lemma 4.11 implies that $a \ker(Tr) = b \ker(Tr)$ if and only if $b = az$ for some $z \in \mathbb{Z}_p$. This implies that there are $\frac{p^n-1}{p-1}$ hyperplanes of the form $a \ker(Tr)$. But, the total number of hyperplanes in $F$ is $\frac{p^n-1}{p-1}$, so every hyperplane has this form. q.e.d.
CHAPTER 5

COMMUTATORS

As was mentioned earlier, commutators will play a large role in the understanding of stabilizers of the characters of our group $G$. To see if an element is in the stabilizer of a character, we need to conjugate that element by another element. The reason that commutators arise is the fact that if we have elements $s$ and $t$, for example, then $t^s = s^{-1}ts = t(t^{-1}s^{-1}ts) = t[t,s]$. Thus, conjugation can be thought of as multiplication on the right by the commutator $[t,s]$.

Rather than attempting to calculate $t^{-1}$ and $s^{-1}$ for use within $[t,s]$, we use the identity $st[t,s] = ts$. With this we will calculate the products $st$, $ts$, and $st[t,s]$. At that point we solve for coefficients of each $x^i$ in $[t,s]$.

Recall that $R$ is the skew polynomial ring with Jacobson radical $J$ and that $P = 1 + J$ and $P^i = 1 + J^i$. Because $J$ is the Jacobson radical of $R$, which is the skew polynomial ring, right multiplication within $P$ is determined by the multiplication within $R$. This is one of the complicating factors of computing $[t,s]$. The other, more complicating factors, are the forms $\langle \cdot, \cdot \rangle_{i,j}$ that appear within the coefficients and how they combine or do not combine with each other.

With all of this in mind we begin this chapter with a result that helps us begin to understand the commutator $[t,s]$ where $s \in P$ and $t \in P^{1+1}$.  


Lemma 5.1 Let \( s = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_q x^q \in P \) and \( t = 1 + \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} + \beta_{\frac{q+3}{2}} x^{\frac{q+3}{2}} + \cdots + \beta_q x^q \in P_{\frac{q+1}{2}} \). Then \([t, s]\) is of the form

\[ 1 + \delta_1 x^{\frac{q+1}{2}} + \delta_2 x^{\frac{q+3}{2}} + \cdots + \delta_{\frac{q-1}{2}} x^q, \]

where

\[ \delta_j = \sum_{i=1}^{j-1} -\alpha_i \beta_{j-i}^p - \sum_{i=1}^{j} \langle \alpha_i, \beta_{j-i} \rangle_{i, j-i} \]

and \( j^* = j + \frac{q+1}{2} \).

Proof. We begin by considering the product \( st \). Write \( t = 1 + y \), where \( y = \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} + \beta_{\frac{q+3}{2}} x^{\frac{q+3}{2}} + \cdots + \beta_q x^q \). We can now think of the product \( st \) as

\[ st = s(1+y) = s + sy. \]

Thus, we will consider the equation

\[ st = s + y + (\alpha_1 x)y + (\alpha_2 x^2)y + \cdots + (\alpha_{q-1} x^{q-1})y + (\alpha_q x^q)y. \]

Define \( j^* = j + \frac{q+1}{2} \) as in the statement of the lemma, where \( 1 \leq j \leq \frac{q-1}{2} \). We now analyze the term from \( st \) that will involve \( x^{j^*} \) for \( \frac{q+3}{2} \leq j^* \leq q \). Notice that this term will result from terms \( \beta_{j^*} x^{j^*} \) added to sums of products of the form \( \alpha_i x^i \beta_{j^*-i} x^{j^*-i} \).

In other words, all of \( y \) except for the first term \( \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} \) will combine with the remaining terms of \( sy \) to form the term we are interested in. Thus, we consider

\[ \beta_{j^*} x^{j^*} + \alpha_1 x \beta_{j^*-1} x^{j^*-1} + \alpha_2 x^2 \beta_{j^*-2} x^{j^*-2} + \cdots + \alpha_{\frac{q-1}{2}} x^{\frac{q-1}{2}} \beta_{j^* - \frac{q-1}{2}} x^{j^* - \frac{q-1}{2}} \]

\[ = \beta_{j^*} x^{j^*} + \alpha_1 \beta_{j^*-1} x^{j^*} + \alpha_2 \beta_{j^*-2} x^{j^*} + \cdots + \alpha_{\frac{q-1}{2}} \beta_{j^* - \frac{q-1}{2}} x^{j^*}. \]
Hence, for the term involving $x_{j^*}$ we can write

$$
\beta_{j^*} x_{j^*} + \alpha_1 \beta_{j^* - 1} x_{j^*} + \alpha_2 \beta_{j^* - 2} x_{j^*} + \cdots + \alpha_{q - 1} \beta_{j^* - \frac{q - 1}{2}} x_{j^*} + \alpha_{q - \frac{q - 1}{2}} \beta_{j^* - \frac{q - 1}{2}} x_{j^*}
$$

$$
= \beta_{j^*} x_{j^*} + \sum_{i=1}^{j^*} \alpha_i \beta_{j^* - i} x_{j^*}.
$$

Summing over all values of $j$ we have that

$$
st = s + \beta_{q + 1} x_{\frac{q + 1}{2}} + \sum_{j=1}^{\frac{q - 1}{2}} \beta_{j^*} x_{j^*} + \sum_{j=1}^{\frac{q - 1}{2}} \sum_{i=1}^{j} \alpha_i \beta_{j^* - i} x_{j^*}.
$$

Now consider the product $ts$. The details provided in the calculation of $st$ should help the reader understand that we can begin by writing

$$
ts = s + y + y(\alpha_1 x) + y(\alpha_2 x^2) + \cdots + y(\alpha_{q - 1} x^{q - 1}) + y(\alpha_q x^q).
$$

Again, we consider the term involving $x_{j^*}$ for $\frac{q + 3}{2} \leq j^* \leq q$. This term will come from $\beta_{j^*} x_{j^*}$ in $y$ added to sums of products of the form $\beta_{j^* - i} x_{j^* - i} \alpha_i x_i$. We see that

$$
\beta_{j^*} x_{j^*} + \beta_{j^* - 1} x_{j^* - 1} \alpha_1 x + \beta_{j^* - 2} x_{j^* - 2} \alpha_2 x^2 + \cdots + \beta_{j^* - \frac{q - 1}{2}} x_{j^* - \frac{q - 1}{2}} \alpha_{\frac{q - 1}{2}} x_{\frac{q - 1}{2}}
$$

$$
= \beta_{j^*} x_{j^*} + \beta_{j^* - 1} \alpha_1 \beta_{j^* - 1} x_{j^*} + \beta_{j^* - 2} \alpha_2 \beta_{j^* - 2} x_{j^*} + \cdots + \beta_{j^* - \frac{q - 1}{2}} \alpha_{\frac{q - 1}{2}} \beta_{j^* - \frac{q - 1}{2}} x_{j^*}.
$$

So for the term involving $x_{j^*}$ in $ts$ we have the summation

$$
\beta_{j^*} x_{j^*} + \sum_{i=1}^{j^*} \alpha_i \beta_{j^* - i} x_{j^*}.
$$
If we sum over all possible values for \( j \) we obtain

\[
 ts = s + \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} + \sum_{j=1}^{\frac{q-1}{2}} \beta_j x^{j^*} + \sum_{j=1}^{\frac{q-1}{2}} \sum_{i=1}^{j} \alpha_i \beta_{j^*} x^{j^*}. 
\]

We now move on to calculate \( st[t,s] \). First, it is straightforward to see that \( [t,s] \) can be written as \( 1 + \delta_1 x^{\frac{q+3}{2}} + \delta_2 x^{\frac{q+5}{2}} + \cdots + \delta_{\frac{q-1}{2}} x^q \). As above, we begin by writing \( [t,s] = 1 + z \) where \( z = \delta_1 x^{\frac{q+3}{2}} + \delta_2 x^{\frac{q+5}{2}} + \cdots + \delta_{\frac{q-1}{2}} x^q \). Thus, from this we see that \( st[t,s] \) can be written

\[
st[t,s] = st + stz = st + (s + \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} + \sum_{j=1}^{\frac{q-1}{2}} \beta_j x^{j^*} + \sum_{j=1}^{\frac{q-1}{2}} \sum_{i=1}^{j} \alpha_i \beta_{j^*} x^{j^*})z. 
\]

Much of the expression on the right side will collapse to zero because the exponent of \( x \) in many terms will exceed \( q \). Consider the expression \( (\beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}})z \). The smallest power of \( x \) here is \( q + 2 \). Thus, the products in that term disappear. Similarly, \( \left( \sum_{j=1}^{\frac{q-1}{2}} \beta_j x^{j^*} \right)z = 0 \) and \( \left( \sum_{j=1}^{\frac{q-1}{2}} \sum_{i=1}^{j} \alpha_i \beta_{j^*} x^{j^*} \right)z = 0 \).

At this point, we now have a much shorter equation to analyze. In other words, we now have

\[
st[t,s] = st + sz.
\]

We now simplify \( sz \) in our equation.

\[
sz = z + \alpha_1 xz + \alpha_2 x^2 z + \cdots + \alpha_{q-1} x^{q-1} z + \alpha_q x^q z.
\]

Consider the term involving \( x^{j^*} \) for \( \frac{q+3}{2} \leq j^* \leq q \). This term will come from \( \delta_j x^{j^*} \) in \( z \) and sums of products of the form \( \alpha_i x^i \delta_{j-i} x^{j^*} \) in the pieces \( \alpha_k x^k z \) for appropriate
values of \( k \). As a result, we see that the term we are interested in is the sum

\[
\delta_j x^j + \alpha_1 x \delta_{j-1} x^{j-1} + \alpha_2 x^2 \delta_{j-2} x^{j-2} + \cdots + \alpha_{\frac{q-3}{2}} x^{\frac{q-3}{2}} \delta_{j-\frac{q-3}{2}} x^{j-\frac{q-3}{2}}
\]

\[
= \delta_j x^j + \alpha_1 \delta_{j-1} x^{j-1} + \alpha_2 \delta_{j-2} x^{j-2} + \cdots + \alpha_{\frac{q-3}{2}} \delta_{j-\frac{q-3}{2}} x^{j-\frac{q-3}{2}}.
\]

Thus, we can summarize our term with the following:

\[
\delta_j x^j + \sum_{i=1}^{j-1} \alpha_i \delta_{j-i} x^{j-i}.
\]

Summing over all values of \( j \) we obtain

\[
\sum_{j=1}^{\frac{q-1}{2}} \delta_j x^j + \sum_{j=1}^{\frac{q-1}{2}} \sum_{i=1}^{j-1} \alpha_i \delta_{j-i} x^{j-i}.
\]

Combining all of these results for \( st[t, s] \), we see that

\[
st[t, s] = s + \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} + \sum_{j=1}^{\frac{q-1}{2}} \beta_j x^j + \sum_{j=1}^{\frac{q-1}{2}} \delta_j x^j + \sum_{j=1}^{\frac{q-1}{2}} \sum_{i=1}^{j} \alpha_i \beta_{j-i} x^{j-i} + \sum_{j=1}^{\frac{q-1}{2}} \sum_{i=1}^{j-1} \alpha_i \delta_{j-i} x^{j-i}.
\]

We now want to compare coefficients of \( x^j \) in both \( st[t, s] \) and \( ts \). Recall that \( st[t, s] = ts \). First notice that since both the left and right sides of this equation have the identical terms \( s + \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}} + \sum_{j=1}^{\frac{q-1}{2}} \beta_j x^j \), these terms cancel. Thus, fixing \( j \) and equating the \( x^j \) terms gives us

\[
\delta_j x^j + \sum_{i=1}^{j-1} \alpha_i \beta_{j-i} x^{j-i} + \sum_{i=1}^{j-1} \alpha_i \delta_{j-i} x^{j-i} = \sum_{i=1}^{j-1} \alpha_i \beta_{j-i} x^{j-i} + \sum_{i=1}^{j-1} \alpha_i \delta_{j-i} x^{j-i}.
\]
If we only compare coefficients from this equation, we see that

\[
\delta_j + \sum_{i=1}^{j} \alpha_i \beta_{j+i} - \sum_{i=1}^{j} \alpha_i \delta_{j-i} = \sum_{i=1}^{j} \alpha_i \beta_{j+i} - \sum_{i=1}^{j} \alpha_i \delta_{j-i}.
\]

Solving for \( \delta_j \) we obtain

\[
\delta_j = -\sum_{i=1}^{j-1} \alpha_i \delta_{j-i} - \sum_{i=1}^{j} \alpha_i \beta_{j+i} + \sum_{i=1}^{j} \alpha_i \beta_{j+i} - \sum_{i=1}^{j} \alpha_i \beta_{j-i}.
\]

For our result, we combine the last two sums and simplify this to

\[
\delta_j = -\sum_{i=1}^{j-1} \alpha_i \delta_{j-i} - \sum_{i=1}^{j} \alpha_i \beta_{j+i} - \sum_{i=1}^{j} \alpha_i \beta_{j-i}.
\]

\[
= -\sum_{i=1}^{j-1} \alpha_i \delta_{j-i} - \sum_{i=1}^{j} \langle \alpha_i, \beta_{j-i} \rangle.
\]

q.e.d.

Though Lemma 5.1 is helpful to the reader to begin to understand the coefficients that arise in the commutator \([t, s]\), we would like to simplify them even further. The main purpose of Lemma 5.1 is to aid in the very technical proof of the next lemma. The next lemma does, in fact, condense the general formula for the coefficients. In other words, by dissecting Lemma 5.1 we are able to recombine the coefficients into a more concise formula. To do this, we certainly incorporate the result from Lemma 5.1. However, we rely very heavily on the results of Lemmas 4.2 and 4.3 for our proof.

**Lemma 5.2** Let \( s \in P \) and \( t \in P^{q+1} \) be defined as in Lemma 5.1. Inductively, we
define $d_1 = \beta_{\frac{q+1}{2}}$. For $k > 1$ define

$$d_k = -\beta_{k^*-1} + \sum_{i=1}^{k-1} \alpha_i (d_{k-i})^{p^i},$$

where $k^* = k + \frac{q+1}{2}$. If we write

$$[t, s] = 1 + \delta_1 x^{\frac{q+3}{2}} + \delta_2 x^{\frac{q+5}{2}} + \cdots + \delta_{q-1} x^q,$$

then $\delta_k = \sum_{i=1}^{k} \langle \alpha_i, d_{k-i+1} \rangle_{i, k^*-i}$.

**Proof.** We proceed by induction on $k$. In the initial case when $k = 1$, we know from Lemma 5.1 that $\delta_1 = -\langle \alpha_1, \beta_{\frac{q+1}{2}} \rangle_{1, \frac{q+1}{2}}$. Hence, the result is true in this case. Suppose that the result holds for all $k = 1, \ldots, m - 1$. By Lemma 5.1 and the induction hypothesis we have the following:

$$\delta_m = -\sum_{i=1}^{m-1} \alpha_i \delta_{m-i}^{p^i} - \sum_{i=1}^{m} \langle \alpha_i, \beta_{m^*-i} \rangle_{i, m^*-i}$$

$$= -\sum_{i=1}^{m-1} \alpha_i \left( \sum_{j=1}^{m-i} \langle \alpha_j, d_{m-i-j+1} \rangle_{j, m^*-i-j} \right)^{p^i} - \sum_{i=1}^{m} \langle \alpha_i, \beta_{m^*-i} \rangle_{i, m^*-i}.$$

We can move $\alpha_i$ inside the inner sum to get

$$\sum_{i=1}^{m-1} \sum_{j=1}^{m-i} \alpha_i (\langle \alpha_j, d_{m-i-j+1} \rangle_{j, m^*-i-j})^{p^i} - \sum_{i=1}^{m} \langle \alpha_i, \beta_{m^*-i} \rangle_{i, m^*-i}.$$ (5.1)

For the moment we will ignore the single summation portion of (5.1) and only work with the double summation. At this point there are two main cases to consider. The two cases are when $i = j$ and when $i \neq j$. We will first consider the easier case when $i = j$. Here we have a sum of products of the form $\alpha_i (\langle \alpha_i, d_{m-2i+1} \rangle_{i, m^*-2i})^{p^i}$. We can
apply Lemma 4.2 to write
\[
\alpha_i(\langle \alpha_i, d_{m-2i+1} \rangle_{i,m^*-2i})^{p^i} = \langle \alpha_i, \alpha_i d_{m-2i+1} \rangle_{i,m^*-i}. \]

Notice that for \( i = j \), we must have \( i \leq m - i \) or \( i \leq \lfloor \frac{m}{2} \rfloor \). Set \( v = \lfloor \frac{m}{2} \rfloor \). So, if we sum over all possible values of \( i \), for each \( i \) we can apply this result to exactly one \( j \). Thus, for our general case we obtain
\[
\alpha_1(\langle \alpha_1, d_{m-1} \rangle_{1,m^*-2})^p + \cdots + \alpha_v(\langle \alpha_v, d_1 \rangle_{v,m^*-2v})^{p^v} = \langle \alpha_1, \alpha_1 d_{m-1} \rangle_{1,m^*-1} + \cdots + \langle \alpha_v, \alpha_v d_{1} \rangle_{v,m^*-v}. \tag{5.2}
\]

We will come back to (5.2) later in the proof when we combine all of our results. For now we move to the case when \( i \neq j \). In order to begin analyzing this more difficult case we will consider when \( i = 1 \) and in essence we argue inductively on \( i \). The reason we choose \( i = 1 \) is not because this is a formal inductive argument, but because this value of \( i \) gives us the maximum number of components for \( j \). The reader will then be able to recognize the pattern more quickly when we sum over all values of \( i \). When \( i = 1 \), the double summation of (5.1) becomes
\[
\sum_{j=1}^{m-1} \alpha_1(\langle \alpha_j, d_{m-j} \rangle_{j,m^*-j-1})^p.
\]

From this, when \( j = 1 \) we pick up the first term in (5.2). Thus, we will do an analysis summing over \( j > 1 \). If we isolate one term and fix \( j = j_0 \), then within this sum we have \( \alpha_1(\langle \alpha_{j_0}, d_{m-j_0} \rangle_{j_0,m^*-j_0-1})^p \). We would like to apply Lemma 4.3 here. To do this we need to combine this term with the term \( \alpha_{j_0}(\langle \alpha_1, d_{m-j_0} \rangle_{1,m^*-j_0-1})^{p_{j_0}} \). Notice that this term comes from the outer summation in (5.1) when \( i = j_0 \). Hence,
in general we will obtain \( m - 2 \) terms of this form that can be combined with the term \( \alpha_1(\langle \alpha_{j_0}, d_{m-j_0} \rangle_{j_0, m^* - j_0 - 1})^p \) using Lemma 4.3. In the specific case that we are considering, if we apply Lemma 4.3, we have

\[
\alpha_1(\langle \alpha_{j_0}, d_{m-j_0} \rangle_{j_0, m^* - j_0 - 1})^p + \alpha_{j_0}(\langle \alpha_1, d_{m-j_0} \rangle_{1, m^* - j_0 - 1})^{p_{j_0}}
\]

\[
= \langle \alpha_1, \alpha_{j_0} d_{m-j_0}^{p_{j_0}} \rangle_{1, m^* - 1} + \langle \alpha_{j_0}, \alpha_1 d_{m-j_0}^{p_{j_0}} \rangle_{j_0, m^* - j_0}.
\]  

(5.3)

We can sum over all possible values for \( j_0 > 1 \) and we get

\[
\sum_{j_0=2}^{m-1}(\langle \alpha_1, \alpha_{j_0} d_{m-j_0}^{p_{j_0}} \rangle_{1, m^* - 1} + \langle \alpha_{j_0}, \alpha_1 d_{m-j_0}^{p_{j_0}} \rangle_{j_0, m^* - j_0}).
\]

Notice that had we fixed \( i = j_0 \) and \( j = 1 \), we would have considered the equation

\[
\alpha_{j_0}(\langle \alpha_1, d_{m-j_0} \rangle_{1, m^* - j_0 - 1})^{p_{j_0}} + \alpha_1(\langle \alpha_{j_0}, d_{m-j_0} \rangle_{j_0, m^* - j_0 - 1})^p
\]

\[
= \langle \alpha_{j_0}, \alpha_1 d_{m-j_0}^{p_{j_0}} \rangle_{j_0, m^* - j_0} + \langle \alpha_1, \alpha_{j_0} d_{m-j_0}^{p_{j_0}} \rangle_{1, m^* - 1}.
\]  

(5.4)

Of course, this term was accounted for already in (5.3). In other words, in general there is some repetition occurring. For example, if we give the label \((a, b)\) to the term

\[
\langle \alpha_a, \alpha_b d_{m-b}^{p_{m-b}} \rangle_{a, m^* - a} + \langle \alpha_b, \alpha_a d_{m-b}^{p_{m-b}} \rangle_{b, m^* - b},
\]

then we will always have \((a, b) = (b, a)\), and hence, a repeated term. Now consider the double summation in (5.1) with \( i = 2 \). We see that summing over all \( j \) we will repeat \((1, 2)\) that was accounted for in (5.3). Hence, fixing \( j = j_0 \) and combining the
appropriate terms we obtain

$$\sum_{j_0=3}^{m-2} (\langle \alpha_2, \alpha_{j_0} d_{m-j_0} \rangle_{2, m^* - 2} + \langle \alpha_{j_0}, \alpha_2 d_{m-j_0} \rangle_{j_0, m^* - j_0}).$$

In general for $i = i_0$, to avoid repeating prior terms we would sum from $j_0 = i_0 + 1$ to $m - i_0$. Now, as $i_0$ increases, so does the starting value for $j_0$ in this sum. Also, as $i_0$ increases, the maximum value for $j_0$ decreases. Thus, the number of terms is decreasing as $i_0$ increases. We must have $i_0 < j_0 \leq m - i_0$. So, $i_0 \leq m - i - 1$ and $2i_0 \leq m - 1$. Thus, we need $i_0 \leq \lfloor \frac{m-1}{2} \rfloor$ for these sums to make sense in general. Set $u = \lfloor \frac{m-1}{2} \rfloor$ and notice that in general we have sums of pairs

$$\langle \alpha_1, \alpha_{j_0} d_{m-j_0} \rangle_{1, m^* - 1} + \langle \alpha_{j_0}, \alpha_1 d_{m-j_0} \rangle_{j_0, m^* - j_0} +$$

$$\cdots + \langle \alpha_u, \alpha_{j_0} d_{m-j_0} \rangle_{u, m^* - u} + \langle \alpha_{j_0}, \alpha_u d_{m-j_0} \rangle_{j_0, m^* - j_0}.$$ 

So, for each of these pairs if we sum over all possible values of $j_0$, we get

$$\sum_{j_0=2}^{m-1} (\langle \alpha_1, \alpha_{j_0} d_{m-j_0} \rangle_{1, m^* - 1} + \langle \alpha_{j_0}, \alpha_1 d_{m-j_0} \rangle_{j_0, m^* - j_0}) +$$

$$\cdots + \sum_{j_0=4}^{m-u} (\langle \alpha_u, \alpha_{j_0} d_{m-j_0} \rangle_{u, m^* - u} + \langle \alpha_{j_0}, \alpha_u d_{m-j_0} \rangle_{j_0, m^* - j_0}).$$

(5.5)

Notice that in the last summation $m - u = u + 1$, so there is only one pair to consider there. Hence, adding (5.2) and (5.5) yields

$$\langle \alpha_1, \alpha_1 d_{m-1} \rangle_{1, m^* - 1} + \cdots + \langle \alpha_v, \alpha_v d_1 \rangle_{v, m^* - v}$$

$$+ \sum_{j_0=2}^{m-1} (\langle \alpha_1, \alpha_{j_0} d_{m-j_0} \rangle_{1, m^* - 1} + \langle \alpha_{j_0}, \alpha_1 d_{m-j_0} \rangle_{j_0, m^* - j_0}).$$
\[
\cdots + \langle \alpha_u, \alpha_{u+1}d_{m-2u}^{m+1} \rangle_{u,m^*-u} + \langle \alpha_{u+1}, \alpha_u d_{m-2u}^m \rangle_{u+1,m^*-u-1}.
\]

Again, we fix \( i = i_0 \) and combine the appropriate terms to form \( \langle \alpha_{i_0}, \cdot \rangle_{i_0, m^*-i_0} \). From (5.6) we see that
\[
\langle \alpha_{i_0}, \cdot \rangle_{i_0, m^*-i_0} = \langle \alpha_{i_0}, \alpha_{i_0}d_{m-i_0}^{m-1} + \alpha_{i_0+1}d_{m-i_0}^{m+1} + \cdots + \alpha_{m-i_0}d_{i_0}^{m-i_0} \rangle_{i_0, m^*-i_0}.
\]

We can now generalize this and sum over all values of \( i \) to get
\[
\sum_{i=1}^{m} \langle \alpha_i, \alpha_{i+1}d_{m-i}^{i+1} + \cdots + \alpha_{m-i}d_{i}^{m-i-1} \rangle_{i,m^*-i} = \sum_{i=1}^{m} \langle \alpha_i, \sum_{j=1}^{m-i} \alpha_j d_{m-j}^{j} \rangle_{i,m^*-i}.
\]

At this point, if we combine the single summation from (5.1) and invoke the induction hypothesis again, we have our desired result
\[
\delta_m = \sum_{i=1}^{m} \langle \alpha_i, -\beta_{m^*-i} + \sum_{j=1}^{m-i} \alpha_j d_{m-j}^{j} \rangle_{i,m^*-i} = \sum_{i=1}^{m} \langle \alpha_i, d_{m-i+1} \rangle_{i,m^*-i}.
\]

q.e.d.

The purpose of the next lemma is to consider a specific case that appears later. The point of the lemma is to show the reader which coefficients disappear within the commutator in this case.

**Lemma 5.3** Assume the notation of Lemma 5.1. Suppose that \( s = 1 + \alpha x^m \). Then

1. \( \delta_j = 0 \) for \( 1 \leq j \leq m-1 \).

2. \( \delta_j = -\langle \alpha, \beta_{j^*-m} \rangle_{m,j^*-m} + \langle \alpha, e \rangle_{m,j^*-m} \) where \( e \) is a polynomial in \( \alpha \) and \( \beta_{\frac{m+1}{2}}, \ldots, \beta_{j^*-m-1} \) when \( m \leq j \leq \frac{n-1}{2} \).
**Proof.** Since the coefficients of $x, x^2, \ldots, x^j$ in $s$ are 0 when $1 \leq j \leq m - 1$, we see from Lemma 5.1 that $\delta_j = 0$ when $1 \leq j \leq m - 1$. Suppose that $m \leq j \leq \frac{q-1}{2}$. Then by Lemma 5.2, we have $\delta_j = \langle \alpha, d_{j-m+1} \rangle_{m,j-m}$ where $d_{j-m+1} = -\beta_{j,m} + \alpha(d_{j-2m})^m$. (We mention here that we write $d_{j-2m} = 0$ if $j - 2m \leq 0$.) It is easy to see that $d_{j-2m}$ is a polynomial in $\alpha$ and $\beta_{j+1}, \ldots, \beta_{j-m-1}$, and so, the result follows. \hspace{1cm} q.e.d.
CHAPTER 6

IRREDUCIBLE CHARACTERS PART I

We begin this chapter by introducing some notation. Let $N$ be a normal subgroup of $G$, and $X$ be a subset of $\text{Irr}(N)$. We define $\text{Irr}(G|X)$ to be the set of characters $\chi \in \text{Irr}(G)$ such that some irreducible constituent of $\chi_N$ lies in $X$. In this spirit, we define $\text{cd}(G|X) = \{\chi(1) | \chi \in \text{Irr}(G|X)\}$. We set $\text{Irr}(G|N) = \text{Irr}(G|X)$ for $X = \text{Irr}(N) \setminus \{1_N\}$ and $\text{cd}(G|N) = \{\chi(1) | \chi \in \text{Irr}(G|N)\}$.

Recall from Chapter 3 that we defined $P^i$ to be $1 + J^i$. Also, recall that $P^i$ is normal in $G$ for any positive integer $i$. Another important fact that comes from Theorem 2.5(i) in [16] is that the group $CP/P^q$ is a Frobenius group with respect to $C$ with Frobenius kernel $P/P^q$. The next lemma provides an alternative proof, to that of Riedl, of this relevant fact.

Lemma 6.1 The group $CP/P^q$ is a Frobenius group with complement $C$ and Frobenius kernel $P/P^q$.

Proof. Let $1 \neq s \in P/P^q$ and $1 \neq c \in C$. Notice that the order of $c$ divides $p^q - 1$. Hence, $c^\frac{p^q - 1}{p^i - 1} \neq 1$ for $i = 1, 2, \ldots, q - 1$. If we write $s = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{q-1} x^{q-1}$, then the previous statement tells us that there exists an $i$ such that $\alpha_i \neq 0$. Therefore, $s \cdot c \neq s$. Thus, $C_{CP/P^q}(c) \leq C$ for all $c \in C$. q.e.d.

There are a few observations that should be mentioned with regard to $CP/P^q$ relative to the fact that it is a Frobenius group. One characteristic is that all proper
nontrivial subgroups of $C$ will complement $P/P^q$. In other words, all subgroups of $C$ are Frobenius complements to $P/P^q$. We also have that for $1 < P^i/P^q < P/P^q$ and $P^i/P^q$ normal in $CP/P^q$, $(CP/P^q)/(P^i/P^q)$ is a Frobenius group with Frobenius kernel $(P/P^q)/(P^i/P^q)$. Also, all normal subgroups of $CP/P^q$ are either contained in $P/P^q$ or contain $P/P^q$ as a subgroup.

Now, the fact that $P/P^q$ is a nontrivial finite $p$-group tells us that $P/P^q$ is nilpotent. In general, though, in any Frobenius group the Frobenius kernel is nilpotent.

The character degrees of $G$ are all contained in the union of the sets $\text{cd}(G/P^q)$ and $\text{cd}(G|P^q)$. This follows from the fact that every irreducible character of $G$ either has $P^q$ in its kernel or does not have $P^q$ in its kernel. We begin by calculating irreducible character degrees of $G/P^q$ and move on to $\text{cd}(G|P^q)$ in the chapters following this one. Most of the work for the proof of the following Lemma can be found in Theorem 4.4 of [16].

**Lemma 6.2** For $P^q$ defined as above, we have

$$\text{cd}(G/P^q) = \left\{ 1, q, r, qr, \left( \frac{p^{qr} - 1}{p - 1} \right) | i = 0, 1, \ldots, q - 2 \right\}.$$ 

**Proof.** To begin computing irreducible character degrees of $G/P^q$, we compute the irreducible character degrees of $G/P \cong C\mathcal{G}$. The Fundamental Theorem of Galois Theory tells us that the intermediate fixed fields correspond to the subgroups of $\mathcal{G}$ via inclusion reversing bijections. So the subgroup of $\mathcal{G}$ of order $q$ corresponds to the fixed field of order $p^r$ and the subgroup of order $r$ in $\mathcal{G}$ corresponds to the fixed field of order $p^q$. In addition, $\mathcal{G}$ corresponds to the fixed field of order $p$. This leads to a correspondence between the subgroups of $F^\times$ and the subgroups of $C$. Viewed as a
The multiplicative group, $C$ is complemented by the subgroup of $F^\times$ of order $p - 1$. Now, $F^\times$ is mapped to $C$ via the map that sends an element $\alpha \in F^\times$ to $\alpha^{p-1}$ in $C$. Hence, $F^\times = C \times \mathbb{C}_{F^\times} (G)$. As a result we see that the subgroup of order $q$ in $G$ centralizes the subgroup of order $\frac{p^q - 1}{p-1}$ in $C$ and thus nonidentity elements of this subgroup lie in orbits of size $r$ under the action of $\mathcal{G}$. The subgroup of order $r$ in $G$ centralizes the subgroup of order $\frac{p - 1}{p^r-1}$ in $C$, and the elements in this subgroup lie in orbits of size $q$. The remaining elements lie in orbits of size $qr$.

Now the character degrees of $G/P$ correspond to the sizes of the orbits of $\mathcal{G}$ acting on $C$. From this, we see that $\text{cd}(G/P) = \{ 1, q, r, qr \}$.

Using Theorem 4.4 of [16] we see that $\text{Irr}(P/P^n)$ contains $p^i(p^{qr} - 1)$ nonprincipal characters of degree $(p^{qr - 1})^i$ for $i = 0, 1, \ldots, q - 2$. Under the action of $C$ these characters lie in orbits of size $\frac{p^{qr - 1}}{p-1}$. It follows that

$$\text{cd}(CP/P^n|P/P^n) = \left\{ \left( \frac{p^{qr - 1}}{p-1} \right)^i \left( \frac{p^{qr} - 1}{p - 1} \right) \mid i = 0, 1, \ldots, q - 2 \right\}.$$ 

Lemma 5.3 in [16], along with Theorem 6.34 in [5] tell us that the conjugacy classes of $P/P^n$ are fixed by $\mathcal{G}$. Thus, each $C$-orbit contains a $\mathcal{G}$-invariant character. So, each $C$-orbit is stabilized by $\mathcal{G}$. Since $\mathcal{G}$ is cyclic, we have $\text{cd}(G/P^n|P/P^n) = \text{cd}(CP/P^n|P/P^n)$. Therefore, at this stage we have shown that

$$\text{cd}(G/P^n) = \left\{ 1, q, r, qr, \left( \frac{p^{qr - 1}}{p-1} \right)^i \left( \frac{p^{qr} - 1}{p - 1} \right) \mid i = 0, 1, \ldots, q - 2 \right\}.$$ 

$q.e.d.$

We mentioned above that $\text{cd}(G) = \text{cd}(G/P^n) \cup \text{cd}(G|P^n)$. Since we have computed $\text{cd}(G/P^n)$, to determine the structure of $\Delta(G)$ we must find $\text{cd}(G|P^n)$. The
character degrees in \( \text{cd}(G|P^q) \) have not been previously computed. As a result, it will require more work and insight than it did to determine the degrees in \( \text{cd}(G/P^q) \).

The remaining chapters are comprised of the results needed to calculate the character degrees in \( \text{cd}(G|P^q) \).
Before we start the main focus of this chapter, we need a small lemma that will be used repeatedly throughout the remainder of this paper.

**Lemma 7.1** Let \( N \) be a normal subgroup of a finite group \( G \). Let \( \lambda \) be a linear character of \( N \). Fix an element \( s \in G \). Then \( s \) stabilizes \( \lambda \) if and only if \( \lambda([t, s]) = 1 \) for all \( t \in N \).

**Proof.** Clearly, \( s \) stabilizes \( \lambda \) if and only if \( s^{-1} \) stabilizes \( \lambda \). Also, \( s \) stabilizes \( \lambda \) if and only if \( (\lambda)^{s^{-1}}(t) = \lambda(t) \) for all \( t \in N \). We know \( (\lambda)^{s^{-1}}(t) = \lambda(t^s) \). Thus, \( s \) stabilizes \( \lambda \) if and only if \( \lambda(t^s) = \lambda(t) \) for all \( t \in N \). We observe that \( \lambda(t^s) = \lambda(t[t, s]) = \lambda(t)\lambda([t, s]) \), as \( \lambda \) is linear. Therefore, \( s \) stabilizes \( \lambda \) if and only if \( \lambda([t, s]) = 1 \) for all \( t \in N \). q.e.d.

Moving on to looking at stabilizers of certain characters of \( P^q \), for \( i \geq \frac{q+1}{2} \) we define the subgroup \( B_i \) of \( P^i \) by \( B_i = \{1 + \alpha x^i | \alpha \in F\} \). Note that

\[
P^{\frac{i+1}{2}} = B_{\frac{i+1}{2}} \times B_{\frac{i+3}{2}} \times \cdots \times B_{\frac{q-1}{2}} \times P_q.
\]

Also, \( B_{\frac{i+1}{2}} \times B_{\frac{i+3}{2}} \times \cdots \times B_{\frac{q-1}{2}} \) is a \( CG \) - invariant subgroup. Characters in \( \text{Irr}(P^{\frac{i+1}{2}}|P^q) \) have the form \( \mu_{\frac{i+1}{2}} \times \mu_{\frac{i+3}{2}} \times \cdots \times \mu_{\frac{q-1}{2}} \times \varphi \), where each \( \mu_i \in \text{Irr}(B_i) \) and \( 1_{P^q} \neq \varphi \in \text{Irr}(P^q) \).
Let $\mathcal{B}$ be the set of characters $\varphi \in \text{Irr}(P^q)$ whose kernels do not correspond to $\langle \alpha, F \rangle_{i,q-i}$ for all $\alpha \in F$ and for $i = 1, 2, \ldots, \frac{q-1}{2}$. Recall that in Corollary 4.8, we saw that the subspaces generated by $\langle \alpha, F \rangle_{i,q-i}$ are independent of $i$. In other words, the sets $\langle \alpha, F \rangle_{1,q-1}$ as $\alpha$ runs through $F$ are the same as $\langle \beta, F \rangle_{i,q-i}$ as $\beta$ runs through $F$.

The next lemma calculates the stabilizer of $\mu_{\frac{q+1}{2}} \times \mu_{\frac{q+3}{2}} \times \cdots \times \mu_{q-1} \times \varphi$ in $P$ when $\varphi \in \mathcal{B}$.

**Lemma 7.2** For $\varphi \in \mathcal{B}$, the stabilizer of $\gamma = \mu_{\frac{q+1}{2}} \times \mu_{\frac{q+3}{2}} \times \cdots \times \mu_{q-1} \times \varphi$ in $P$ is $P^{\frac{q+1}{2}}$. As a result, $\varphi$ is fully ramified with respect to $P/P^q$ and $\gamma^P$ is irreducible.

**Proof.** Fix an element $s \in P - P^{\frac{q+1}{2}}$. We need to show that $s$ does not stabilize $\gamma$. From Lemma 7.1, we see that it suffices to show that there exists an element $t \in P^{\frac{q+1}{2}}$ so that $\gamma([t, s]) \neq 1$. We can write $s = 1 + \alpha x^i + y$, where $0 \neq \alpha \in F$, $1 \leq i \leq \frac{q-1}{2}$, and $y \in J^{i+1}$. Since the kernel of $\varphi$ does not correspond to $\langle \alpha, F \rangle_{i,q-i}$, we can find $\beta \in F$, so that $1 + \langle \alpha, \beta \rangle_{i,q-i} x^q \notin \ker(\varphi)$. Let $t = 1 + \beta x^{q-i} + z$, where $z \in J^{q-i+1}$. From Lemma 4.1 in [6], we know that $[t, s] = 1 + \langle \alpha, \beta \rangle_{i,q-i} x^q$. Hence,

$$
\gamma(1 + \langle \alpha, \beta \rangle_{i,q-i} x^q) = \varphi(1 + \langle \alpha, \beta \rangle_{i,q-i} x^q) \neq 1.
$$

Thus, when $\varphi \in \mathcal{B}$ we have that $P^{\frac{q+1}{2}}$ is the stabilizer of $\gamma$ in $P$. In particular, by Theorem 6.11 of [5], $\gamma^P$ is irreducible. As a result, $\varphi$ is fully ramified with respect to $P/P^q$. q.e.d.

Now, define $C_q$ to be the subgroup of $C$ of order $\frac{p^q-1}{p-1}$. This subgroup will be used throughout the remainder of the paper.

**Lemma 7.3** For $\mathcal{B}$ defined as above, we have $\text{cd}(G|\mathcal{B}) = \{ q^{\frac{q^r-1}{p^r-1}} (\frac{p^r-1}{p-1}) \}$. 
Proof. From Lemma 7.2, we conclude that the characters in $\text{Irr}(P|B)$ all have degree $p^{\frac{q^r-1}{q^r-1}}$. Let $C_q$ be the subgroup defined above and let $D_q$ be the complement to $C_q$ in $C$. Now, $C_q$ centralizes $P^q$, and since the characters in $\text{Irr}(P|P^q)$ are fully ramified with respect to $P/P^q$, it follows that $C_q$ centralizes these characters. On the other hand, $D_q$ acts Frobeniously on $P^q$, so nonprincipal characters in $\text{Irr}(P^q)$ all lie in orbits of $D_q$. Hence, characters in $\text{Irr}(P|P^q)$ all lie in regular orbits of size $p^{\frac{q^r-1}{q^r-1}}$ under the action of $C$. We deduce that $\text{Irr}(CP|B)$ consists of characters of degree $p^{\frac{q^r-1}{q^r-1}}(p^{q^r-1} - p^{q-1})$.

We know from Lemma 4.12 every hyperplane in $F$ has the form $a\text{ker}(Tr)$ for some $0 \neq a \in F$. For $c \in C$, the action of $C$ on the hyperplanes of $P^q$ is

$$\{1 + \beta x^q \mid \beta \in \text{aker}(Tr)\} \cdot c = \{1 + \beta e^{\frac{p^q-1}{p^r-1}} x^q \mid \beta \in \text{aker}(Tr)\}.$$  

Similarly, for $\sigma \in G$, the action of $G$ on the hyperplanes in $P^q$ is

$$\{1 + \beta x^q \mid \beta \in \text{aker}(Tr)\} \cdot \sigma = \{1 + \beta^\sigma x^q \mid \beta \in \text{aker}(Tr)\}.$$  

Thus, the orbits of hyperplanes under the action of $C$ correspond to cosets of $D_q$ in $C$. Since the elements of order $r$ in $G$ centralize $C_q$, this implies the elements of order $r$ in $G$ will stabilize each orbit of hyperplanes. The only hyperplanes fixed by the elements of order $q$ in $G$ will be those of the form $\{1 + \beta x^q \mid \beta \in \text{aker}(Tr)\}$, where $o(a)$ divides $\frac{p^r-1}{p-1}$. It is not difficult to see that none of these correspond to characters in $B$. Thus, $G$ will permute the hyperplanes corresponding to characters in $B$ in orbits of size $q$. Different characters in the same $CG$-orbit must have different kernels, so the action on the hyperplanes will translate to the action on the characters. Thus, $q$ divides the size of every orbit under the action of $G$ on $\text{Irr}(CP|B)$. Since the subgroup
of order $r$ in $\mathcal{G}$ centralizes $C_q$, we conclude that $\text{cd}(G|\mathcal{B}) = \{q p^{\frac{q-1}{2}} r^r (\frac{p^r - 1}{p - 1})\}$. q.e.d.
IRREDUCIBLE CHARACTERS PART III

We now focus our attention on those characters $\varphi \in \text{Irr}(P^q)$ whose kernels correspond to $\langle \alpha, F \rangle_{i,q-i}$ for some $\alpha \in F$ and some $1 \leq i \leq \frac{q-1}{2}$. Define $A$ to be this set of characters. Notice that $A$ is a union of $p - 1$ orbits of size $\frac{p^{qr-1}}{p(qr-1)}$ under the action of $C$. Each $C$-orbit contains a character whose kernel corresponds to $\ker(Tr)$.

Fix $\varphi \in \text{Irr}(P^q)$ so that $\ker(\varphi) = \{1 + \alpha x^q \mid \alpha \in \ker(Tr)\}$. Thus, there is a one-to-one correspondence between $\ker(\varphi)$ and $\ker(Tr)$. The reader at times may find it to be more convenient to think of $\ker(\varphi)$ as the $\ker(Tr)$, or in other words, to view $\varphi$ as a character of $F$.

Now set $A_{\frac{q+1}{2}}$ to be the $P$-orbit in $\text{Irr}(P^{\frac{q+1}{2}})$ that contains $1_{B_{\frac{q+1}{2}}} \times 1_{B_{\frac{q+3}{2}}} \times \cdots \times 1_{B_{q-1}} \times \varphi$.

As we will see later there are other characters of this form to consider. Specifically, we need to analyze characters in other $P$-orbits where certain $\mu_i \neq 1_{B_i}$. Many of the calculations that emerge begin to get complicated and require various approaches to determine stabilizers. The characters in this chapter, however, are relatively speaking much easier to work with.

To begin our lemmas we need a couple of definitions. First, we define $F_q$ be the field of order $p^q$. Next, define $Q$ to be the set of all elements $1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_q x^q$ where each $\alpha_i$ lies in $F_q$. We will show in the following lemma that this subgroup plays
a role in the stabilizers of certain representative characters of $A_{q-1}$.

**Lemma 8.1** Set $\gamma = \mu_{q+1}^+ \times 1_{B_{q+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi$, where $\mu_{q+1}^+ \in \text{Irr}(B_{q+1})$. Then the stabilizer in $P$ of $\gamma$ is the subgroup $QP_{q+1}^+$. 

**Proof.** First, we will show that elements of $QP_{q+1}^+$ stabilize $\gamma$. Choose an element $s \in QP_{q+1}^+$. We saw in Lemma 7.1 that it suffices to show that $\gamma([t, s]) = 1$ for all $t \in P_{q+1}^+$. Write $s = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_q x^q$ and $t = 1 + \beta_{q+1}^+ x^{q+1} + \beta_{q+2} x^{q+2} + \cdots + \beta_q x^q$, where $\alpha_1, \ldots, \alpha_{q-1} \in F_q$ and $\alpha_{q+1}, \ldots, \alpha_q, \beta_{q+1}, \ldots, \beta_q \in F$. We know from Lemma 5.2 that the coefficients of $x^j$ in $[t, s]$ can be written $\sum_{i=1}^{q-1} \langle \alpha_{j-q-1}, d_{j-q-1} \rangle_i, j^*, j^* - i$ where $d_k = -\beta_{k^*} + \sum_{l=1}^{k} \alpha_l (d_{k-l})^{p^l}$, and $k^* = k + \frac{q+1}{2}$. Thus, we can write

$$[t, s] = 1 + \sum_{j=\frac{q+1}{2}}^{q-1} \sum_{i=1}^{q-1} \langle \alpha_{j-q-1}, d_{j-q-1} \rangle_i, j^*, j^* - i x^j.$$ 

Now, $\gamma([t, s]) = 1$ if and only if $\varphi(1 + \sum_{i=1}^{q-1} \langle \alpha_{j-q-1}, d_{j-q-1} \rangle_i, q-i x^q) = 1$. By definition of $\langle \cdot, \cdot \rangle_{i, q-i}$, we have

$$\text{Tr}(\sum_{i=1}^{q-1} \langle \alpha_{j-q-1}, d_{j-q-1} \rangle_{i, q-i}) = \text{Tr}(\sum_{i=1}^{q-1} (\alpha_{q-1} d_{q-1}^{p^i} - \alpha_{q-1} d_{q-1}^{p^i})).$$

Using the linearity of the trace map, we obtain

$$\text{Tr}(\sum_{i=1}^{q-1} (\alpha_{q-1} d_{q-1}^{p^i} - \alpha_{q-1} d_{q-1}^{p^i} - \alpha_{q-1} d_{q-1}^{p^i})) = \sum_{i=1}^{q-1} (\text{Tr}(\alpha_{q-1} d_{q-1}^{p^i}) - \text{Tr}(\alpha_{q-1} d_{q-1}^{p^i})).$$

Since $\text{Tr}(a^p) = \text{Tr}(a)$ for all $a \in F$, we have

$$\text{Tr}(\alpha_{q-1} d_{q-1}^{p^i}) = \text{Tr}(\alpha_{q-1} d_{q-1}^{p^i} p^i) = \text{Tr}(\alpha_{q-1} d_{q-1}^{p^i} d_{q-1}^{p^i}).$$
Because $\alpha_{q-1} \in F_q$, we know that $\alpha_{q-1}^q = \alpha_{q-1}$, so we have $Tr(\alpha_{q-1}^{p^i} d_{q-1}^{p^i}) = Tr(\alpha_{q-1}^{p^i} z_{q-1}^{p^i})$. This yields

$$\sum_{i=1}^{q-1} Tr(\alpha_{q-1}^{p^i} d_{q-1}^{p^i} - \alpha_{q-1}^{p^i} z_{q-1}^{p^i}) = \sum_{i=1}^{q-1} (Tr(\alpha_{q-1}^{p^i} d_{q-1}^{p^i}) - Tr(\alpha_{q-1}^{p^i} z_{q-1}^{p^i})) = 0.$$  

We conclude that

$$\sum_{i=1}^{q-1} \langle \alpha_{q-1}^{p^i}, d_{q-1}^{p^i} \rangle_{q-1} \in \ker(Tr)$$

and hence, $1 + \sum_{i=1}^{q-1} \langle \alpha_{q-1}^{p^i}, d_{q-1}^{p^i} \rangle_{q-1} x^q \in \ker(\varphi)$. Therefore, $\gamma([s, t]) = 1$ as desired. Thus, $QP^{q+1}$ is contained in the stabilizer of $\gamma$.

We now work to show that $QP^{q+1}$ is the stabilizer of $\gamma$. Consider an element $s \in P - QP^{q+1}$. We will show that $s$ does not stabilize $\gamma$. By Lemma 7.1, it suffices to find $t \in P^{q+1}$ so that $\gamma([t, s]) \neq 1$. Now $\varphi$ was chosen so that $\ker(\varphi) = \{1 + \alpha x^q \mid \alpha \in \ker(Tr)\}$. We know from Lemma 4.5 that $\ker(Tr) = \langle \alpha, F \rangle_{i,q-1}$ if and only if $\alpha \in F_q$. There are two cases to consider. First consider the case when $s = 1 + \alpha x^i + y$, where $\alpha \notin F_q$ and $y \in J^{i+1}$. Then we can choose $\beta \notin F_q$ so that $\langle \alpha, \beta \rangle_{i,q-1} \notin \ker(Tr)$. Let $t = 1 + \beta x^{q-i}$, so that $[t, s] = 1 + \langle \alpha, \beta \rangle_{i,q-1} x^q$. Since $\langle \alpha, \beta \rangle_{i,q-1} \notin \ker(Tr), [t, s] \notin \ker(\varphi)$ as desired.

Secondly, consider the case when $s = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_x x^i + y$ where $\alpha_1, \ldots, \alpha_{i-1} \in F_q, \alpha_i \notin F_q$, and $y \in J^{i+1}$. Write $r = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{i-1} x^{i-1}$ for $r \in QP^{q+1}$ and $z = r^{-1}(y - (r - 1)\alpha_i x^i) \in J^{i+1}$. Then

$$r(1 + \alpha_i x^i + z) = r + r\alpha_i x^i + (y - (r - 1)\alpha_i x^i)$$

$$= r + \alpha_i x^i + y = s.$$
Also, notice that \( z = r^{-1}(y + \alpha_i x^i) - \alpha_i x^i \in J^{i+1} \). Thus, we can write \( s = rw \) where \( r \in QP^{z+i} \) and \( w = 1 + \alpha_i x^i + z \). Since \( \alpha_i \notin F_q \), the previous paragraph shows \( w \) cannot be in the stabilizer of \( \gamma \). Hence, \( s \) is not in the stabilizer of \( \gamma \). Therefore, the only elements in \( P \) that stabilize \( \gamma \) are the elements in \( QP^{z+i} \).

\[ q.e.d. \]

Using a technique similar to that found in [9], the next lemma helps us understand the characters in \( A_{q+1} \). The main difference between the argument below and the one used by Lewis is that we now use induction since we have more than one factor group to consider.

**Lemma 8.2** The character \( 1_{B_{q+1}^{z+i}} \times 1_{B_{q+1}^{z+i+1}} \times \cdots \times 1_{B_{q-1}^{z+i}} \times \varphi \) has a unique \( C_q \)-invariant extension to \( QP^{z+i} \).

**Proof.** Set \( Q^i = P_i \cap QP^{z+i} \). Observe that \( Q^1 = QP^{z+i} \) and \( Q^{i+1} = P^{z+i} \). We will use reverse induction to prove that \( \gamma_{i+1} = 1_{B_{q+1}^{z+i}} \times \cdots \times 1_{B_{q-1}^{z+i}} \times \varphi \) has a unique \( C_q \)-invariant extension to \( Q^1 \). Since \( \gamma_{z+i} \) is the only extension of \( \gamma_{z+i} \) to \( Q^{z+i} \) and is \( C_q \)-invariant, the base case holds. Now suppose that \( 1 \leq i \leq q-1 \) and \( \gamma_{z+i} \) has a unique \( C_q \)-invariant extension \( \gamma_{i+1} \) to \( Q^{i+1} \). We know that \( Q^i/Q^{i+1} \) is irreducible under the action of \( C_q \), so by Problem 6.12 of [5], we know that either \( \gamma_{i+1} \) extends to \( Q^i \) or is fully ramified with respect to \( Q^i/Q^{i+1} \). Since \( |Q^i : Q^{i+1}| = p^i \) is not a square, \( \gamma_{i+1} \) is not fully ramified with respect to \( Q^i/Q^{i+1} \). Thus, \( \gamma_{i+1} \) extends to \( Q^i \).

By Glauberman’s Lemma, Lemma 13.8 in [5], \( \gamma_{i+1} \) has a \( C_q \)-invariant extension to \( Q^i \). On the other hand, by the corollary to Glauberman’s Lemma, Corollary 13.9 in [5], we know that \( C_{Q^i/Q^{i+1}}(C_q) \) acts transitively on the \( C_q \)-invariant extensions of \( \gamma_{i+1} \) to \( Q^i \). Since \( C_{Q^i/Q^{i+1}}(C_q) = 1 \), it follows that \( \gamma_{i+1} \) has a unique \( C_q \)-invariant extension \( \gamma_i \) to \( Q^i \). It follows that \( \gamma_{z+i} \) will extend to \( Q^i \), and since any \( C_q \)-invariant
For $\phi$ in $[16]$. Gallagher’s Theorem tells us that there is a bijection from $\text{Irr}(\mathbb{C})$ to $\mathbb{Q}$. Taking $i = 1$, we have the desired result. 

$q.e.d.$

We now have enough information to produce the character degrees of $\text{cd}(G \mid A_{\frac{q-1}{2}})$.

**Lemma 8.3** For $A_{\frac{q-1}{2}}$ defined as above, we have $\text{cd}(G \mid A_{\frac{q-1}{2}}) = \left\{ p^{\left(\frac{q-1}{2}\right)(q^r-q)} \left( \frac{p^r-1}{p^r-1} \right), q^{\left(\frac{q-1}{2}\right)(q^r-1)} \left( \frac{p^r-1}{p^r-1} \right), p^{\left(\frac{q-1}{2}\right)(q^r-q+i)} \left( \frac{p^r-1}{p^r-1} \right) \mid i = 0, 1, \ldots, \frac{q-3}{2} \right\}$.

**Proof.** Recall, $C_q$ is the subgroup of $C$ of order $\frac{p^r-1}{p-1}$. From Lemma 8.2 we know there is a unique $C_q$-invariant subgroup of $\gamma = 1_{B_{\frac{q-1}{2}}} \times 1_{B_{\frac{q+3}{2}}} \times \ldots \times 1_{B_{q-1}} \times \phi$ to $QP^{\frac{q^r}{2}}$. Call this character $\hat{\phi} \in \text{Irr}(QP^{\frac{q^r}{2}})$. By Theorem 6.11 in [5], $\hat{\phi}$ induces irreducibly to $P$. Since $\phi$ is linear, it has degree 1. Now, $\hat{\phi}^P$ is a $C_q$-invariant irreducible character of $P$ whose degree is equal to $|P : QP^{\frac{q^r}{2}}|$, which is $p^{\left(\frac{q-1}{2}\right)(q^r-q)}$. In particular, $\hat{\phi}^P$ is stabilized by $PC_q$, and using Corollary 6.28 from [5], it has $\frac{p^r-1}{p-1}$ extensions to $PC_q$. These characters also have degree $p^{\left(\frac{q-1}{2}\right)(q^r-q)}$. From here, our characters induce irreducibly to $CP$ with degree $p^{\left(\frac{q-1}{2}\right)(q^r-q)} \left( \frac{p^r-1}{p^r-1} \right)$. Now, from earlier comments on the action of $G$, we know that $G$ stabilizes one of these characters and permutes the rest in orbits of size $q$. As a result, we see that this yields character degrees in $\text{cd}(G \mid A_{\frac{q-1}{2}})$ of $p^{\left(\frac{q-1}{2}\right)(q^r-q)} \left( \frac{p^r-1}{p^r-1} \right)$ and $q^{\left(\frac{q-1}{2}\right)(q^r-1)} \left( \frac{p^r-1}{p^r-1} \right)$.

For the remaining characters in $\text{Irr}(QP^{\frac{q^r}{2}} \mid \gamma)$ that are not the unique $C_q$-invariant extension $\hat{\phi}$ in $QP^{\frac{q^r}{2}}$, notice that $QP^{\frac{q^r}{2}} / P^{\frac{q^r}{2}}$ is one of the groups studied in [16]. Gallagher’s Theorem tells us that there is a bijection from $\text{Irr}(QP^{\frac{q^r}{2}} / P^{\frac{q^r}{2}})$ to $\text{Irr}(QP^{\frac{q^r}{2}} \mid \gamma)$. The degrees of the characters in $\text{Irr}(QP^{\frac{q^r}{2}} / P^{\frac{q^r}{2}})$ were computed in Theorem 4.4 of [16]. From there, we see that, excluding the unique $C_q$-invariant extension, in $\text{Irr}(QP^{\frac{q^r}{2}})$ we have $p^r(p^r-1)$ characters of degree $p^{\left(\frac{q-1}{2}\right)}$ for $i = 0, 1, \ldots, \frac{q-3}{2}$. Again, via Theorem 6.11 in [5], each of these characters induces irreducibly to $P$.
with degree $p^{i(q-1)/2}p^{(q-1)/2}(qr-q) = p^{i(q-1)/2}(qr-q+i)$ for $i = 1, 2, \ldots, \frac{q-3}{2}$. Since $C$ permutes these characters in orbits of size $\frac{pqr-1}{p-1}$, these characters induce irreducibly to $CP$. Thus, we see in $\text{Irr}(CP \mid A_{q-1})$, these characters have degrees $p^{i(q-1)/2}(qr-q+i)\left(\frac{p^{q-1}}{p-1}\right)$ for $i = 1, 2, \ldots, \frac{q-3}{2}$. Notice that $G$ stabilizes these characters, so each extends to $G$.

Therefore, we have $\text{cd}(G \mid A_{q-1}) = \{p^{(q-1)/2}(qr-q)\left(\frac{p^{q-1}}{p-1}\right), q\left(\frac{p^{q-1}}{p-1}\right), p^{i(q-1)/2}(qr-q+i)\left(\frac{p^{q-1}}{p-1}\right) \mid i = 0, 1, \ldots, \frac{q-3}{2}\}$. q.e.d.

Now, $A_{\frac{q-1}{2}}$ was defined to be the $P$-orbit in $\text{Irr}(P_{\frac{q+1}{2}})$ that contains $1_{B_{\frac{q+1}{2}}} \times 1_{B_{\frac{q+3}{2}}} \times \cdots \times 1_{B_{q-1}} \times \varphi$, where $\varphi$ is a fixed irreducible character of $P^q$ whose kernel corresponds to the kernel of the trace map. We continue with $\varphi$ fixed and we now define $A_{\frac{q+1}{2}}$ to be the $P$-orbits in $\text{Irr}(P_{\frac{q+1}{2}})$ that contain characters of the form $\mu_{\frac{q+1}{2}} \times 1_{B_{\frac{q+3}{2}}} \times \cdots \times 1_{B_{q-1}} \times \varphi$ but nothing in $A_{\frac{q-1}{2}}$.

Before we move on to the next lemma, we first provide a definition of certain characters in $B_i$. Recall that $P^q \cong B_i \cong F$. Thus, characters of $B_i$ can be thought of as characters of $F$ or characters of $P^q$. With this in mind, given $\alpha \in F$ and an integer $i \geq 1$, we define $\varphi_{\alpha}^{i,q-i} \in \text{Irr}(B_{q-i})$ by

$$\varphi_{\alpha}^{i,q-i}(1 + \beta x^{q-i}) = \varphi(1 + \langle \alpha, \beta \rangle_{i,q-i} x^q).$$

We will show in Lemma 8.5 that this map is, in fact a homomorphism. We need an additional definition for the next lemma. We define $B_{q-i,q} = \{1 + \beta x^{q-i} \mid \beta \in F_q\}$.

The importance of this set is its relationship to the kernel of the map above.

**Lemma 8.4** Fix $\alpha \in F$ and $i \geq \frac{q+1}{2}$. Then $B_{q-i,q} \subseteq \ker(\varphi_{\alpha}^{i,q-i})$ for all $i$ and for all $\alpha \in F$. 

Proof. Let $\beta \in F_q$. Using the linearity of the trace map,

$$\text{Tr}((\alpha, \beta)_{i,q-i}) = \text{Tr}(\alpha \beta^p - \alpha^{p^{q-i}} \beta) = \text{Tr}(\alpha \beta^p) - \text{Tr}(\alpha^{p^{q-i}} \beta).$$

Since $\text{Tr}(a^p) = \text{Tr}(a)$ for all $a \in F$, we have

$$\text{Tr}(\alpha \beta^p) = \text{Tr}((\alpha \beta^p)^{p^{q-i}}) = \text{Tr}(\alpha^{p^{q-i}} \beta^p).$$

Hence,

$$\text{Tr}(\alpha \beta^p - \alpha^{p^{q-i}} \beta) = \text{Tr}(\alpha^{p^{q-i}} \beta^p - \alpha^{p^{q-i}} \beta) = \text{Tr}(\alpha^{p^{q-i}} \beta^p - \alpha^{p^{q-i}} \beta).$$

Because $\beta \in F_q$, we obtain $\beta^{p^q} = \beta$ and thus,

$$\text{Tr}(\alpha^{p^{q-i}} \beta^p - \alpha^{p^{q-i}} \beta) = \text{Tr}(\alpha^{p^{q-i}} \beta - \alpha^{p^{q-i}} \beta) = \text{Tr}(0) = 0.$$

We combine these to obtain $\text{Tr}((\alpha, \beta)_{i,q-i}) = 0$. We now see that $\varphi_i^{q-i}(1 + \beta x^{q-i}) = \varphi(1 + \langle \alpha, \beta \rangle_{i,q-i} x^q) = 1$ since $\ker(\varphi) = \{1 + \alpha x^q | \alpha \in \ker(\text{Tr})\}$ and $\langle \alpha, \beta \rangle_{i,q-i} \in \ker(\text{Tr})$. We conclude that $B_{q-i,q} \subseteq \ker(\varphi_i^{q-i})$. q.e.d.

In order to determine any character degrees in $\text{cd}(G \mid A_{q+1})$, it will be useful to have the following lemma. In this lemma, we will show that the map $\alpha \mapsto \varphi_i^{q-i}$ is a homomorphism, and we will determine its image and kernel. This will help us identify the degrees in $\text{cd}(G \mid A_{q+1}).$

Lemma 8.5 Define the map $*: F \longrightarrow \text{Irr}(B_{q-i})$ by $\alpha \mapsto \varphi_i^{q-i}$. Then $*$ is a homomorphism with kernel $F_q$ and image $\text{Irr}(B_{q-i}/B_{q-i,q})$.  

Proof. For $\alpha, \beta \in F$ we have

$$
\varphi_{\alpha+\beta}^{i,q^{-i}}(1 + \gamma x^{q^{-i}}) = \varphi(1 + \langle \alpha + \beta, \gamma \rangle_{i,q^{-i}}x^q)
$$

$$
= \varphi(1 + \langle \alpha, \gamma \rangle_{i,q^{-i}} x^q) \varphi(1 + \langle \beta, \gamma \rangle_{i,q^{-i}} x^q)
$$

since $\langle \cdot, \cdot \rangle_{i,q^{-i}}$ is bilinear and $\varphi$ is a homomorphism, and

$$
\varphi(1 + \langle \alpha, \gamma \rangle_{i,q^{-i}} x^q) \varphi(1 + \langle \beta, \gamma \rangle_{i,q^{-i}} x^q) = \varphi_{\alpha}^{i,q^{-i}}(1 + \gamma x^{q^{-i}}) \varphi_{\beta}^{i,q^{-i}}(1 + \gamma x^{q^{-i}})
$$

by definition of $\varphi_{\alpha}^{i,q^{-i}}$. Thus $\ast$ is a homomorphism. By Lemma 8.4, $Im(\ast) \subseteq Irr(B_{q^{-i}}/B_{q^{-i},q})$. If $\alpha \in F_q$, then

$$
Tr(\langle \alpha, \beta \rangle_{i,q^{-i}}) = Tr(\alpha \beta^{p^i} - \alpha^{p^{q^{-i}}} \beta) = Tr(\alpha \beta^{p^i}) - Tr(\alpha^{p^{q^{-i}}} \beta).
$$

We know that $Tr(\alpha^{p^{q^{-i}}} \beta) = Tr((\alpha^{p^{q^{-i}}} \beta)^{p^i}) = Tr(\alpha^{p^{q^{-i}}} \beta^{p^i})$. Since $\alpha \in F_q$, $\alpha^{p^i} = \alpha$ so $Tr(\alpha^{p^{q^{-i}}} \beta) - Tr(\alpha \beta^{p^i}) = 0$. Thus, $\alpha \in ker(\ast)$, and $F_q \subseteq ker(\ast)$.

If $\alpha \in ker(\ast)$, then $\varphi_{\alpha}^{i,q^{-i}} = 1$. This implies $\varphi_{\alpha}^{i,q^{-i}}(1 + \beta x^{q^{-i}}) = 1$ for all $\beta \in F$. We see that $\varphi(1 + \langle \alpha, \beta \rangle_{i,q^{-i}} x^q) = 1$ and hence $\langle \alpha, \beta \rangle_{i,q^{-i}} \in ker(Tr)$ for all $\beta \in F$, which implies $\alpha \in F_q$ by Lemma 4.5. Therefore, $F_q = ker(\ast)$, so $|ker(\ast)| = p^i$, and

$$
|Im(\ast)| = \frac{|F|}{|ker(\ast)|} = \frac{p^{qr}}{p^i} = p^{qr-q} = |Irr(B_{q-i}/B_{q-i,q})|.
$$

We conclude that $\ast$ maps onto $Irr(B_{q-i}/B_{q-i,q})$. q.e.d.
CHAPTER 9

A SPECIFIC EXAMPLE

In this chapter we will demonstrate some of the structure of the group we will call $G_3$ that will be constructed based on fixing the prime $q = 3$. The primes $p$ and $r$ will be general, but will satisfy the necessary parameters outlined in the beginning of this paper. In the case when $q = 3$, the character degrees arise relatively easily. When we move up from this case to $q > 3$ the character degrees become more difficult to obtain, as we will see in the next chapter. In this chapter, we show that one character degree in addition to previous ones appears for irreducible characters in $A_{q+1},$ where $A_{q+1}$ is defined as in the previous chapter. Specifically, with $q = 3$ this will be $A_2$. The reader will see that this additional degree will not change the diameter of the character degree graph of our group $G$.

In order to obtain the additional character degree, we need one more lemma before we can demonstrate what occurs when $q = 3$. This next lemma will be extended later to general $A_i$, but is needed here before we go further. Recall $B_{\frac{q+1}{2}} = \{ 1 + \beta x^{\frac{q+1}{2}} | \beta \in F_q \}$. This is a special subgroup that is needed again in the next chapter. Notice in the case when $q = 3$, we have $B_{2,3} = \{ 1 + \beta x^2 | \beta \in F_3 \}$.

**Lemma 9.1** For $A_{\frac{q+1}{2}}$ defined as above,

$$\text{cd}(G | A_{\frac{q+1}{2}}) = \left\{ p^{\frac{q+1}{2}}(q^r - q^{\frac{r+1}{2}}) \left( \frac{p^r - 1}{p - 1} \right) \right\}.$$  

68
Proof. Fix $0 \neq \alpha \in F$. Suppose $s = 1 + \alpha x^{q+1}$ and $t = 1 + \beta x^{q+1} + \cdots + \beta x^q \in P^{q+1}$. Let $\gamma = \mu x^{q+1} \times 1_{B_{q+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi$. We next consider $\gamma^{-1}(t) = \gamma(t^s) = \gamma(t)\gamma([t, s])$. Thus, it suffices to determine $\gamma([t, s])$. Also, from Lemma 5.3 we know that $[t, s] = 1 + (\alpha, \beta x^{q+1})_{q+1} x^q$. Hence, $\gamma([t, s]) = \varphi(1 + (\alpha, \beta x^{q+1})_{q+1} x^q)$. Now, by definition of $\varphi$, we have that

$$\gamma(1 + (\alpha, \beta x^{q+1})_{q+1} x^q) = \varphi_{\alpha, \beta x^{q+1}}(1 + \beta x^{q+1} x^{q+1}).$$

Then

$$(\gamma)^{-1} = (\mu x^{q+1} \times 1_{B_{q+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi) \cdot (\varphi_{\alpha, \beta x^{q+1}} \times 1_{B_{q+1}} \times \cdots \times 1_{F}).$$

Thus, we have

$$(\gamma)^{-1} = \varphi_{\alpha, \beta x^{q+1}} \times 1_{B_{q+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi.$$

Recall $B_{q+1} = \{1 + \beta x^{q+1} \mid \beta \in F\}$. By Lemma 8.5, we know that going through all possible choices of $\alpha \in F$, then $\varphi_{\alpha q^{-1}, \beta x^{q+1}}$ runs through all characters in $\text{Irr}(B_{q+1} / B_{q+1} \cdot q)$ in $\text{Irr}(B_{q+1})$. Define $D_{q+1} = \{1 + \beta x^{q+1} \mid \beta \in [F, \sigma]\}$. Since $F = F_q + [F, \sigma]$, $B_{q+1} \cong F$, and $B_{q+1} \cdot q \cong F_q$, we have that $B_{q+1} = B_{q+1} \cdot q + D_{q+1}$. Hence $\text{Irr}(B_{q+1}) = \text{Irr}(B_{q+1} / B_{q+1} \cdot q) \times \text{Irr}(B_{q+1} / D_{q+1} \cdot q)$, and the coset $\mu_{\beta x^{q+1}} \text{Irr}(B_{q+1} / B_{q+1} \cdot q)$ contains a unique character $\hat{\mu}_{\beta x^{q+1}} \in \text{Irr}(B_{q+1} / D_{q+1} \cdot q)$, where $D_{q+1} \cdot q \subseteq \text{ker}(\hat{\mu}_{\beta x^{q+1}})$. Observe that $A_{q+1}$ consists of the orbits identified with the cosets $\mu_{\beta x^{q+1}} \text{Irr}(B_{q+1} / B_{q+1} \cdot q)$ where $B_{q+1} \cdot q \not\subseteq \text{ker}(\mu_{\beta x^{q+1}})$. Hence, $\gamma$ is conjugate to $\hat{\gamma} = \hat{\mu}_{\beta x^{q+1}} \times 1_{B_{q+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi$ in $A_{q+1}$.

We define $Q^i = P^i \cap Q$, which is different from the definition of $Q^i$ in Lemma
8.2. From Lemma 8.1, we know that the stabilizer in $P$ of $\hat{\gamma}$ is $QP^{a+1}$. Now, $\hat{\mu}_q \times 1_{B^{a+1}} \times \cdots \times 1_{B_q} \in \text{Irr}(P^{a+1}/(D_{a+1}^q + P^{a+1}))$ and by Lemma 8.2, $\hat{\gamma}^{Q_{a+1}} = 1_{B^{a+1}} \times 1_{B^{a+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi$ extends to $QP^{a+1}$. Since $B^{a+1} = B^{a+1}_q + D^{a+1}_q$, we have

$$P^{a+1}_{q+1} = \frac{B^{a+1}_{q+1}}{P^{a+1}_{q+1}} + \frac{D^{a+1}_{q+1}}{P^{a+1}_{q+1}}.$$ 

We also know that $Q \cap B^{a+1} = B^{a+1}_q$. Thus, we have $QP^{a+1}/(D^{a+1}_q + P^{a+1}) \cong Q/Q^{a+1}$. With this in mind, we apply Gallagher’s Theorem to see $\text{Irr}(Q/Q^{a+1})$ is in bijection with $\text{Irr}(QP^{a+1}/\hat{\gamma})$. Hence, we can view characters in $\text{Irr}(QP^{a+1}/\hat{\gamma})$ as characters in $\text{Irr}(Q/Q^{a+1} | \hat{\mu}_q)$. Notice that $Q/Q^{a+1}$ is one of the groups studied by Riedl in [16].

Using Riedl’s results, we have that the characters in $\text{Irr}(Q/Q^{a+1} | Q^{a+1}/Q^{a+1})$ all have degree $p^{(a+1)(a+1)}$. Thus, the characters in $\text{Irr}(QP^{a+1}/\hat{\gamma})$ will all have degree $p^{(a+1)(a+1)}$. Using Clifford theory, these induce irreducibly to $P$ of degree $p^{(a+1)(a+1)}(q^r - q + \frac{1}{2})$. As we saw in the proof of Lemma 8.3, under the action of $C$, these characters are permuted in orbits of size $\frac{p^r-1}{p-1}$ and hence, induce irreducibly to $CP$. So, for characters in $\text{Irr}(CP | A^{a+1})$, the degree of each is $p^{(a+1)(q^r - q + \frac{1}{2})}(\frac{p^r-1}{p-1})$.

Now, $G$ stabilizes each of these characters. Thus, we have

$$\text{cd}(G | A^{a+1}) = \left\{ p^{(a+1)(q^r - q + \frac{1}{2})}(\frac{p^r-1}{p-1}) \right\}.$$ 

$q.e.d.$

At this point we have enough results to calculate the character degrees for the case when $q = 3$. We choose $p$ to be any prime and choose $r > 3$ so that 3 and $r$ do not divide $\frac{p^r-1}{p-1}$. 


We begin by recalling the construction of these groups. To construct \(G_3\) we see that our field \(F\) now has order \(p^{3r}\) and the ring \(R\) is obtained by factoring out the ideal generated by \(X^4\). The subgroup \(P\) is the set of all elements \(1 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3\), where \(\alpha_i \in F\) for \(i = 1, 2, 3\). There are \(p^{3r}\) choices for each \(\alpha_i\) so that \(|P| = p^{9r}\). We take \(C\) to be the subgroup of \(F^\times\) of order \(\frac{p^{3r-1}}{p-1}\) and \(T\) to be the semidirect product of \(C\) acting on \(P\), by the somewhat nonstandard action by automorphisms defined in Chapter 3. Lastly, our group \(G_3\) is then completed by taking the semidirect product of \(G\), the Galois group of \(F\) over the prime subfield, acting on \(T\). In the end, \(G_3\) has order \(3rp^{9r}(\frac{p^{3r-1}}{p-1})\) which, as was mentioned earlier, is very large even if \(p = 2\).

A point to make here is that when we consider the groups \(P_i = 1 + J_i\) for purposes of calculating character degrees, we have the same number of subgroups \(P_i\) as in [9]. In particular, the stabilizers of the characters in [9] were found to be the groups \(P^2\) and \(QP^2\). The key is the group \(P^{\frac{q+1}{2}}\) and where it lies relative to \(P\), which in turn depends on the value of \(q\). In other words, the number of groups \(P^i\) that contain \(P^{\frac{q+1}{2}}\) and are contained in \(P\) directly affects the difficulty of calculating the character degrees. The reader will be able to see this more clearly in the next chapter.

We proceed in the order of previous chapters and we now look to the character degrees of \(G_3/P^3\). Using the result from Lemma 6.2, we have that

\[
\text{cd}(G_3/P^3) = \left\{ 1, p, 3, r, 3r, \frac{p^{3r}-1}{p-1}, p, \frac{3r-1}{2}, \left(\frac{p^{3r}-1}{p-1}\right) \right\}.
\]

We now partition the nonprincipal characters of \(\text{Irr}(P^3)\) into two sets. We will let \(A\) be the set of \(\varphi \in \text{Irr}(P^3)\) whose kernels correspond to \(\langle \alpha, F \rangle_{1,2}\) for some \(0 \neq \alpha \in F\), and we will let \(B\) be the remaining nonprincipal characters in \(\text{Irr}(P^3)\).
Define $B_2 = \{1 + \beta x^2 \mid \beta \in F\}$, which is a subgroup of $P^2$. Also notice that, as in [9], $P^2 = B_2 \times P^3$. Characters in $\text{Irr}(P^2 \mid P^3)$ have the form $\mu_2 \times \varphi$ where $\mu_2 \in \text{Irr}(B_2)$ and $1_{P^3} \neq \varphi \in \text{Irr}(P^3)$.

From Lemma 7.2, with $\varphi \in B$, we know that the stabilizer in $P$ of $\mu_2 \times \varphi$ is $P^2$. In particular, $\varphi$ is fully ramified with respect to $P/P^3$ and $(\mu_2 \times \varphi)^P$ is irreducible. Applying Lemma 7.3, we have that $\text{cd}(G_3|B) = \{3p^{3r}(\frac{p^{3r}-1}{p-1})\}$.

Recalling the definition of $A$, we set $A_1$ to be the $P$-orbit in $\text{Irr}(P^2)$ that contains $1_B \times \varphi$, where $\varphi \notin B$. It is worthwhile to remind the reader that by Lemma 8.1, we know the stabilizer of $1_B \times \varphi$ is the subgroup $QP^2$, as in [9], and as we mentioned above. The character degrees in $\text{cd}(G_3|A_1)$, using Lemma 8.3, are known to be

$$\text{cd}(G_3 \mid A_1) = \left\{p^{3r-3} \left(\frac{p^{3r}-1}{p^3-1}\right), 3p^{3r-3} \left(\frac{p^{3r}-1}{p^3-1}\right), p^{3r-3} \left(\frac{p^{3r}-1}{p-1}\right)\right\}.$$ 

Lastly, we define $A_2$ to be the $P$-orbits in $\text{Irr}(P^2)$ that contain characters of the form $\mu_2 \times \varphi$ but contain nothing from $A_1$. Again, we mention by Lemma 8.1, we know that the stabilizer in $P$ of $\mu_2 \times \varphi$ is $QP^2$. By Lemma 9.1, we have

$$\text{cd}(G_3 \mid A_2) = \left\{p^{3r-2} \left(\frac{p^{3r}-1}{p-1}\right)\right\}.$$ 

We need to confirm one more piece of necessary information before we combine our character degrees. We claim that $\text{cd}(G \mid A) = \text{cd}(G \mid A_1) \cup \text{cd}(G \mid A_2)$. Given the character $\mu_2 \times \varphi$, let $s = 1 + \alpha x$ and $t = 1 + \beta_2 x^2 + \beta_3 x^3$. Consider $(\mu_2 \times \varphi)^s(t)$.

We know $(\mu_2 \times \varphi)^s(t) = (\mu_2 \times \varphi)(t^s) = (\mu_2 \times \varphi)(t[t, s]) = (\mu_2 \times \varphi)(t)(\mu_2 \times \varphi)([t, s])$. 


Using an argument similar to that in [9], we have

\[(\mu_2 \times \varphi)(t)(\mu_2 \times \varphi)([t, s]) = (\mu_2 \times \varphi)((1 + \beta_2 x^2 + (\beta_3 + \langle \alpha, \beta_2 \rangle_1, 2)x^3)\]

\[= \mu_2(1 + \beta_2 x^2)\varphi(1 + (\beta_3 + \langle \alpha, \beta_2 \rangle_1, 2)x^3).\]

On the other hand

\[(\mu_2\varphi^2_\alpha \times \varphi)(t) = \mu_2\varphi^2_\alpha(1 + \beta_2 x^2)\varphi(1 + \beta_3 x^3)\]

\[= \mu_2(1 + \beta_2 x^2)\varphi(1 + (\beta_3 + \langle \alpha, \beta_2 \rangle_1, 2)x^3).\]

From this we see that \(s\) stabilizes \(\mu_2 \times \varphi\) if and only if \(\varphi^2_\alpha = 1_{B_2}\). This occurs only if \(\ker(\varphi) = \{1 + \beta x^3|\beta \in \langle \alpha, F \rangle_1, 2\}\). If \(\mu_2 = 1_{B_2}\) then \(\mu_2 \times \varphi \in A_1\). Otherwise \(\mu_2 \times \varphi \in A_2\).

Combining all of these results, we have

\[
\text{cd}(G_3) = \left\{1, 3, r, 3r, \frac{p^{3r} - 1}{p - 1}, \frac{p^{3r} - 1}{p - 1}, 3p^{3r} - 3, p^{3r} - 3, \frac{p^{3r} - 1}{p^3 - 1}\right\},
\]

Though we do not show the character degree graph here, there are some points worth mentioning. Notice that \(p, q,\) and \(r\) are prime divisors of degrees in \(\text{cd}(G_3)\). In order to determine the remaining primes in \(\rho(G_3)\), we need to determine the primes that divide \(\frac{p^{3r} - 1}{p - 1}\) and \(\frac{p^{3r} - 1}{p^3 - 1}\). In Chapter 10 we will discuss these sets of primes in the general case, as well as which vertices they represent in the graph \(\Delta(G)\). The graph
we show there can be easily applied to the case when $q = 3$.

Many of the techniques used to conquer the case when $q = 3$ can be attributed to Lewis in [9], who partly employed results of Riedl’s in [16]. Thus, this specific example discussed here is relatively straightforward, as was expected. Moving beyond this example to $q > 3$, however, takes much more effort to prove. Patterns do emerge that make it possible to prove the general case. However, alternative techniques are required to identify these patterns and get the desired result.
IRREDUCIBLE CHARACTERS PART IV

For this chapter we continue to focus on characters in $\mathcal{A}$. However, we will study characters not in $\mathcal{A}_{q^{-1}}$ or $\mathcal{A}_{q+1}$. The characters we will look at will be characters of the form

$$\theta = \mu_{q+1} \times \mu_{q+3} \times \cdots \times \mu_{q-1} \times \varphi,$$

where $\mu_i \in \text{Irr}(B_i)$ and $1 \neq \varphi \in \text{Irr}(P^q)$ is such that $\ker(\varphi) = \{1 + \alpha x^q | \alpha \in \ker(Tr)\}$.

Recall we chose $\sigma \in \mathcal{G}$ such that the order of $\sigma$ is $r$. We should also remind the reader that the majority of the results of this chapter only apply to cases when the prime $q$ is larger than 3.

Lemma 10.1 Fix $i, j \in \mathbb{Z}^+$ so that $i + j < q$. If $\alpha \in F_q$, then $\langle \alpha, [F; \sigma] \rangle_{i,j} = [F, \sigma]$ and $\langle \alpha, F \rangle_{i,j} = \langle \alpha, F_q \rangle_{i,j} + [F, \sigma]$.

Proof. Note that by Fitting’s lemma, $F = \mathbb{C}_F(\sigma) + [F, \sigma]$ and $\mathbb{C}_F(\sigma) = F_q$, so $F = F_q + [F, \sigma]$. Consider

$$\langle \alpha, F \rangle_{i,j} = \langle \alpha, F_q + [F, \sigma] \rangle_{i,j} = \langle \alpha, F_q \rangle_{i,j} + \langle \alpha, [F, \sigma] \rangle_{i,j}.$$
Now, $\langle \alpha, F_q \rangle_{i,j} \subseteq F_q$ since $\alpha \in F_q$. Also, $[F, \sigma] = \{ \gamma - \gamma^p | \gamma \in F \}$. We now show that $\langle \alpha, [F, \sigma] \rangle_{i,j} \subseteq [F, \sigma]$. Using the bilinearity of $\langle \cdot, \cdot \rangle_{i,j}$ we have

$$\langle \alpha, \gamma - \gamma^p \rangle_{i,j} = \langle \alpha, \gamma \rangle_{i,j} - \langle \alpha, \gamma^p \rangle_{i,j}.$$ 

Since $\alpha \in F_q$, we can write

$$\langle \alpha, \gamma \rangle_{i,j} - \langle \alpha, \gamma^p \rangle_{i,j} = \langle \alpha, \gamma \rangle_{i,j} - \langle \alpha^p, \gamma^p \rangle_{i,j}.$$ 

And finally, since $F$ has characteristic $p$, we have

$$\langle \alpha, \gamma \rangle_{i,j} - \langle \alpha^p, \gamma^p \rangle_{i,j} = \langle \alpha, \gamma \rangle_{i,j} - (\langle \alpha, \gamma \rangle_{i,j})^p \in [F, \sigma].$$ 

Since $\langle \alpha, F_q \rangle_{i,j} \subseteq F_q$, $\langle \alpha, [F, \sigma] \rangle_{i,j} \subseteq [F, \sigma]$, and $F_q \cap [F, \sigma] = 1$, we know that

$$\langle \alpha, F \rangle_{i,j} = \langle \alpha, F_q \rangle_{i,j} + \langle \alpha, [F, \sigma] \rangle_{i,j}.$$ 

Next, notice that

$$\langle \alpha, F \rangle_{i,j} = \langle \alpha, F_q \rangle_{i,j} + \langle \alpha, [F, \sigma] \rangle_{i,j} \subseteq \langle \alpha, F_q \rangle_{i,j} + [F, \sigma].$$ 

Since $\langle \alpha, F_q \rangle_{i,j}$ is a hyperplane in $F_q$, by Lemma 4.5, it follows that $\langle \alpha, F_q \rangle_{i,j} + [F, \sigma]$ is a hyperplane in $F_q + [F, \sigma] = F$. We also know by Lemma 4.5 that $\langle \alpha, F \rangle_{i,j}$ is a hyperplane in $F$. Hence, we must have equality. Therefore, $\langle \alpha, F \rangle_{i,j} = \langle \alpha, F_q \rangle_{i,j} + [F, \sigma]$ and $\langle \alpha, [F, \sigma] \rangle_{i,j} = [F, \sigma]$. 

$q.e.d.$
Given $\alpha \in F$, positive integers $i$ and $j$, and $\mu_{i+j} \in \text{Irr}(B_{i+j})$ we define $(\mu_{i+j})^{i,j}_{\alpha} \in \text{Irr}(B_j)$ by
\[
(\mu_{i+j})^{i,j}_{\alpha}(1 + \beta x^j) = \mu_{i+j}(1 + \langle \alpha, \beta \rangle_{i,j} x^{i+j}).
\]
Notice the differences between this definition and $\varphi^{i,q-i}_{\alpha}$ defined in Chapter 8.

**Lemma 10.2** Fix $i, j \in \mathbb{Z}^+$ so that $\frac{q+1}{2} \leq i + j \leq q-1$ and fix $\alpha \in F_q$. Choose $c \in \mathbb{Z}^+$ so that $c \equiv (p^i - 1)^{-1} \text{mod}(o(\alpha))$. Set $b \equiv c(p^j - 1) \text{mod}(o(\alpha))$. Let $\mu_{i+j} \in \text{Irr}(B_{i+j})$ such that $\ker(\mu_{i+j}) = \{1 + \beta x^{i+j} \mid \beta \in \langle \alpha, F \rangle_{i,j}\}$. Define $\ast : F_q \rightarrow \text{Irr}(B_j)$ by
\[
\ast(\gamma) = (\mu_{i+j})^{i,j}_{\gamma}.
\]
Then $\ast$ is a homomorphism with kernel $\alpha \mathbb{Z}_p$ and image $\text{Irr}(B_j/E)$, where $E = \{1 + \beta x^j \mid \beta \in \alpha^b \mathbb{Z}_p + [F, \sigma]\}$.

**Proof.** Let $\gamma_1, \gamma_2 \in F_q$. By definition,
\[
\ast(\gamma_1 + \gamma_2)(\cdot) = (\mu_{i+j})^{i,j}_{\gamma_1} + (\mu_{i+j})^{i,j}_{\gamma_2}(\cdot) = \mu_{i+j}(1 + \langle \gamma_1 + \gamma_2, \cdot \rangle_{i,j} x^{i+j}).
\]
Since $\mu_{i+j}$ is itself a homomorphism, we have
\[
\mu_{i+j}(1 + \langle \gamma_1 + \gamma_2, \cdot \rangle_{i,j} x^{i+j}) = \mu_{i+j}(1 + \langle \gamma_1, \cdot \rangle_{i,j} x^{i+j}) \mu_{i+j}(1 + \langle \gamma_2, \cdot \rangle_{i,j} x^{i+j}).
\]
Again, by definition of $\ast$, we have
\[
\mu_{i+j}(1 + \langle \gamma_1, \cdot \rangle_{i,j} x^{i+j}) \mu_{i+j}(1 + \langle \gamma_2, \cdot \rangle_{i,j} x^{i+j}) = \ast(\gamma_1) \ast(\gamma_2).
\]
Thus, $\ast$ is a homomorphism.

We now determine the kernel of $\ast$. Let $\beta \in \alpha \mathbb{Z}_p$. Then
\[
\ast(\beta)(\cdot) = (\mu_{i+j})^{i,j}_{\beta}(\cdot) = \mu_{i+j}(1 + \langle \beta, \cdot \rangle_{i,j} x^{i+j}).
\]
Since $\beta \in \alpha \mathbb{Z}_p$, we have that $1 + \langle \beta, \cdot \rangle x^{i+j} \in \ker(\mu_{i+j})$. Hence $\alpha \mathbb{Z}_p \subseteq \ker(*)$.

On the other hand, let $0 \neq \beta \in \ker(*)$. Then

$$\ast(\beta)(\cdot) = (\mu_{i+j})_{\beta}^{i+j}(\cdot) = \mu_{i+j}(1 + \langle \beta, \cdot \rangle x^{i+j}) = 1.$$ 

This implies that $\langle \beta, F \rangle_{i,j} \subseteq \langle \alpha, F \rangle_{i,j}$. Since these are both hyperplanes in $F$, we must have equality. Thus, $\beta \in \alpha \mathbb{Z}_p$. With containment both directions we have $\ker(*) = \alpha \mathbb{Z}_p$.

We know by Lemma 4.6 that $\langle \alpha, F \rangle_{i,j} = \alpha \mathbb{Z}_p^{i+j-1} \ker(Tr)$. By the same lemma we know $\langle F, \alpha^b \rangle_{i,j} = \alpha \mathbb{Z}_p^{i+j-1} \ker(Tr)$. Thus, there exists $\gamma \in F$ such that $\langle \gamma, \alpha^b \rangle_{i,j} = \langle \alpha, \gamma \rangle_{i,j}$. As a result,

$$(\mu_i)^{i,j}_\gamma(1 + \alpha^b x^j) = \mu_i(1 + \langle \gamma, \alpha^b \rangle_{i,j} x^{i+j}) = \mu_i(1 + \langle \alpha, \gamma \rangle_{i,j} x^{i+j}) = 1.$$ 

Hence, $\{1 + \beta x^{i+j} \mid \beta \in \alpha \mathbb{Z}_p \} \subseteq \ker((\mu_{i+j})_{\gamma}^{i,j})$. Also, we have chosen $\mu_{i+j}$ so that $\ker(\mu_{i+j}) = \{1 + \beta x^{i+j} \mid \beta \in \langle \alpha, F \rangle_{i+j} \}$. Notice that by Lemma 10.2, this is equivalent to saying that $\{1 + \beta x^{i+j} \mid \beta \in [F, \sigma] \} \subseteq \ker(\mu_{i+j})$. By Lemma 10.1, this implies that $\{1 + \beta x^{i+j} \mid \beta \in [F, \sigma] \} \subseteq \ker((\mu_{i+j})_{\alpha}^{i,j})$.

Comparing the sizes of $F_q/\alpha \mathbb{Z}_p$ and $\text{Irr}(B_j/E)$, we see that $| F_q : \alpha \mathbb{Z}_p | = p^{q-1}$. On the other hand

$$| \text{Irr}(B_j/E) | = | B_j : E | = \left| \frac{F}{\alpha \mathbb{Z}_p + [F, \sigma]} \right|.$$ 

Recall that $F_q \cong F/[F, \sigma]$ which, of course, has size $p^q$. This combined with the fact that $| \alpha \mathbb{Z}_p | = p$, we have $| F : \alpha^b \mathbb{Z}_p + [F, \sigma] | = p^{q-1}$. Therefore, by the First Isomorphism Theorem, our map $\ast$ is an isomorphism with image $\text{Irr}(B_j/E)$. q.e.d.
The importance of this next lemma is to be able to characterize \( F_q \) in terms of hyperplanes. This will become a useful tool when it comes to finding the character degrees.

**Lemma 10.3** Fix \( i \in \mathbb{Z}^+ \) so that \( \frac{q+1}{2} \leq i \leq q-1 \) and fix \( \alpha \in F_q \) so that \( o(\alpha) \) divides \( \frac{\nu^2-1}{p-1} \). Let \( b = \frac{\nu^2-1}{p-1} \). Then \( F_q = \alpha^b \mathbb{Z}_p + \langle \alpha, F_q \rangle_{1,i-1} \).

**Proof.** Within this proof we now denote \( Tr \) for the trace map from \( F_q \) to \( \mathbb{Z}_p \). Since \( \langle \alpha, F_q \rangle_{1,i-1} \) is a hyperplane in \( F_q \) and \( \alpha^b \mathbb{Z}_p \) has order \( p \), it suffices to prove that \( \alpha^b \) does not lie in \( \langle \alpha, F_q \rangle_{1,i-1} \). By Lemma 4.7, \( \langle \alpha, F_q \rangle_{1,i-1} = \alpha^{i-1} \ker(Tr) = \alpha^b \ker(Tr) \), where we consider \( Tr \) to be the trace map on \( F_q \). We need to show that \( \alpha^b \) is not in \( \alpha^b \ker(Tr) \), which is equivalent to showing that 1 is not in \( \ker(Tr) \). We see that \( Tr(1) = q \) and since \( p \) does not divide \( q \), we have \( 1 \notin \ker(Tr) \). Therefore, \( \alpha^b \notin \alpha^b \ker(Tr) \). \( \text{q.e.d.} \)

Alternatively, in the proof of Lemma 10.3 we could have compared the size of \( F_q \) to that of \( \alpha^b \mathbb{Z}_p + \langle \alpha, F_q \rangle_{i,j-1} \) to show that this is a direct sum.

In order to determine stabilizers of the characters we are studying in this chapter, we need to calculate conjugates of those characters. Thus, we need a way to characterize these conjugates. The next two lemmas rely on results in Chapter 5 to make this calculation much simpler.

**Lemma 10.4** Let \( \gamma = \mu_{q+1} \times \mu_{q+2} \times \cdots \times \mu_{q-1} \times \varphi \), where \( \mu_i \in \text{Irr}(B_i) \) for \( i = \frac{q+1}{2}, \ldots, q-1 \), and let \( s = 1 + \alpha x^m \) with \( \alpha \in F \) and \( 1 \leq m \leq \frac{q-1}{2} \). Then

\[
\gamma^{s^{-1}} = \gamma \cdot (\nu_{q+1} \times \nu_{q+2} \times \cdots \times \nu_{q-m-1} \times \varphi_{\alpha}^{m,q-m} \times 1_{B_{q-m+1}} \times \cdots \times 1_{B})
\]

where \( \nu_i \in \text{Irr}(B_i) \).
Proof. Consider \( t \in P^{q+1}_{q-1} \). We know that \( \gamma^{s^{-1}}(t) = \gamma(t^s) = \gamma(t[s]) = \gamma(t)\gamma([t, s]) \), since \( \gamma \) is linear. Thus, it suffices to compute \( \gamma([t, s]) \). We write \( t \) as in Lemma 5.1. Using notation from Lemma 5.1 for \([t, s]\), we have

\[
\gamma([t, s]) = \mu_{q+1}^2 (1 + \delta_1 x^{q+1}_2) \mu_{q+2} (1 + \delta_2 x^{q+3}_2) \cdots \mu_{q-1} (1 + \delta_{q-3} x^{q-1}_2) \varphi(1 + \delta_{q-1} x^q).
\]

By Lemma 5.3, we see for \( i = 1, 2, \ldots, q-1 \) that \( \delta_i \) has the form \( \langle \alpha, d_{q-i+1}, q-i \rangle \) where \( d_{q-i+1} \) is a polynomial in \( \alpha \) and \( \beta_{q+i-1}, \ldots, \beta_{q-m-1} \). Also by Lemma 5.3, \( \delta_{q-1} = \langle \alpha, \beta_{q-m}, q-m \rangle + e \) where \( e \) is also a polynomial in \( \alpha \) and \( \beta_{q+i-1}, \ldots, \beta_{q-m-1} \). Thus, \( \gamma([t, s]) \) will be the product of various characters defined over \( \beta_{q+i-1}, \ldots, \beta_{q-m-1} \) times \( \varphi(1 + \langle \alpha, \beta_{q-m}, q-m \rangle) \). Gathering together the like terms, we obtain

\[
\gamma([t, s]) = \nu_{q+1} (1 + \beta_{q+1} x^{q+1}_2) \cdots \nu_{q-m-1} (1 + \beta_{q-m-1} x^{q-m-1}_2) \varphi_{\alpha \beta_{q-m}} (1 + \beta_{q-m} x^{q-m}),
\]

for some characters \( \nu_i \in \text{Irr}(B_i) \). Since \( \gamma^{s^{-1}}(t) = \gamma(t)\gamma([t, s]) \), we have

\[
\gamma^{s^{-1}} = \gamma \cdot (\nu_{q+1} \times \nu_{q+3} \times \cdots \times \nu_{q-m-1} \times \varphi_{\alpha \beta_{q-m}} \times 1_{B_{q-m+1}} \times \cdots \times 1_{P_i}),
\]

where \( \nu_i \in \text{Irr}(B_i) \). q.e.d.

Lemma 10.5 Let \( \gamma = \mu_{q+1} \times \cdots \times \mu_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi \), where \( \mu_j \in \text{Irr}(B_j) \) for \( j = q+1, \ldots, i \), and let \( s = 1 + \alpha x^m \) with \( \alpha \in F_q \) and \( 1 \leq m \leq \frac{q-1}{2} \). Then

\[
\gamma^{s^{-1}} = \gamma \cdot (\nu_{q+1} \times \nu_{q+3} \times \cdots \times \nu_{i-m-1} \times (\mu_i)^{m-i-m} \times 1_{B_{i-m+1}} \cdots \times 1_{P_i}),
\]

for some characters \( \nu_j \in \text{Irr}(B_j) \).
**Proof.** Consider \( t \in P_{\frac{q+1}{2}} \). We saw in the proof of Lemma 10.4 that it suffices to compute \( \gamma([t, s]) \) since \( \gamma^{s-1}(t) = \gamma(t)\gamma([t, s]) \). Write \( t \) as in Lemma 5.1. Using the notation from Lemma 5.1 for \([t, s]\), we have

\[
\gamma([t, s]) = \mu_{\frac{q+1}{2}}(1 + \delta_1 x^{\frac{q+1}{2}})\mu_{\frac{q+3}{2}}(1 + \delta_2 x^{\frac{q+3}{2}}) \cdots \mu_i(1 + \delta_{i-\frac{2}{q}} x^i)\phi(1 + \delta_{\frac{2}{q}-1} x^q).
\]

By Lemma 5.3, we have that \( \delta_{\frac{q-1}{2}} = (\alpha, d_{q-m+1})_{m,q-m} \). Since \( \alpha \in F_q \), we know that \( 1 + (\alpha, d_{q-m+1})_{m,q-m} x^q \in \ker(\phi) \). We have \( \gamma([t, s]) = \mu_{\frac{q+1}{2}}(1 + \delta_1 x^{\frac{q+1}{2}}) \cdots \mu_i(1 + \delta_{i-\frac{2}{q}} x^i) \). Now, \( \delta_1, \ldots, \delta_{i-\frac{2}{q}} \) are polynomials in \( \alpha \) and \( \beta_1, \ldots, \beta_{i-1} \) and \( \delta_{i-\frac{2}{q}} \) is \( (\alpha, \beta_{i-1})_{m,i-m} + e \), where \( e \) is a polynomial in the same variables. Thus, \( \gamma([t, s]) \) will be the product of various characters defined over \( \beta_{\frac{q+1}{2}}, \ldots, \beta_{i-1} \) times \( \mu_i(1 + (\alpha, \beta_{i-1})_{m,i-m} x^i) \). Gathering together the like terms, we obtain

\[
\gamma([t, s]) = \nu_{\frac{q+1}{2}}(1 + \beta_{\frac{q+1}{2}} x^{\frac{q+1}{2}}) \cdots \nu_{i-1}(1 + \beta_{i-1} x^{q-1}) \mu_{i,m-i} \mu_{i,m} \mu_1 \cdots \mu_{p_i},
\]

for some characters \( \nu_j \in \text{Irr}(B_i) \). Again, since \( \gamma^{s-1}(t) = \gamma(t)\gamma([t, s]) \), we have

\[
\gamma^{s-1} = \gamma \cdot \nu_{\frac{q+1}{2}} \times \nu_{\frac{q+3}{2}} \times \cdots \times \nu_{i-1} \times (\mu_i)^{m-i-m} \times 1_{B_{i-1}} \times \cdots \times 1_{p_i}.
\]

for some characters \( \nu_j \in \text{Irr}(B_j) \). \( q.e.d. \)

Recall by the definitions of \( B_{q-i} \) and \( B_{q-i,q} \), we can say that \( B_{q-i} \cong F_q \) and \( B_{q-i,q} \cong F_q \). We also know that \( F = F_q + [F, \sigma] \). Thus, \( B_{q-i,q} \) is complemented in \( B_{q-i} \). This leads us to define \( D_{q-i,q} = \{1 + \beta x^{q-1} \mid \beta \in [F, \sigma]\} \). Using this we can write \( B_{q-i} = B_{q-i,q} \uplus D_{q-i,q} \). We use this fact in proving the next lemma.

**Lemma 10.6** Fix \( i \in \mathbb{Z}^+ \) with \( \frac{q+1}{2} \leq i \leq q - 1 \) and \( \alpha \in F_q \) so that \( o(\alpha) \mid \frac{q^{i-1}}{p-1} \). Suppose \( \mu_i \in \text{Irr}(B_i) \) such that \( \ker(\mu_i) = \{1 + \beta x^i \mid \beta \in [\alpha, F]\}_{1,i-1} \). Let \( \theta \in \text{Irr}(P_{\frac{q+1}{2}}) \).
with
\[ \theta = \mu_{\frac{q+1}{2}} \times \cdots \times \mu_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi. \]

Then \( \theta \) is conjugate to
\[ \hat{\mu}_{\frac{q+1}{2}} \times \cdots \times \hat{\mu}_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi, \]
where \( \{1 + \beta x^l \mid \beta \in \langle \alpha, F \rangle_{1,l-1} \} \subseteq \ker(\hat{\mu}_l) \) for \( l = \frac{q+1}{2}, \frac{q+3}{2}, \ldots, i-1 \), and \( \hat{\mu}_i = \mu_i \).

**Proof.** We find a sequence of characters \( \theta_1 = \theta, \theta_2, \ldots, \theta_i \) so that
\[ \theta_j = \mu_{\frac{j+1}{2}}^{x+1} \times \cdots \times \mu_{i-j}^{x+1} \times \hat{\mu}_{i-j+1} \times \cdots \times \hat{\mu}_i \times 1_{B_{i+1}} \cdots \times 1_{B_{q-1}} \times \varphi, \]
where \( \mu_l \in \text{Irr}(B_l) \) for \( l = \frac{q+1}{2}, \ldots, i-1 \). For \( j = 1, \ldots, i-1 \), we show that \( \theta_j \) is \( P \)-conjugate to \( \theta_{j+1} \). By the transitivity of conjugacy, this will show that \( \theta \) is \( P \)-conjugate to \( \theta_i \), which has the desired form.

We consider \( \theta_j \), and we look at \( s_1 = 1 + \gamma x^{q-i+j} \) for any element \( \gamma \in F \). We will fix \( \gamma \) later. By Lemma 10.4, we have that
\[ (\theta_j)^{s_1^{-1}} = \theta_j \cdot (\nu_{\frac{j+1}{2}}^{x+1} \times \cdots \times \nu_{i-j-1}^{x+1} \times \varphi^{q-i+j,i-j} \times 1_{B_{i-j+1}} \times \cdots \times 1_{p_q}). \]

Writing out the components of \( \theta_j \), we see that
\[ (\theta_j)^{s_1^{-1}} = \mu_{\frac{j+1}{2}}^{x+1} \nu_{\frac{j+1}{2}}^{x+1} \times \cdots \times \mu_{i-j-1}^{x+1} \nu_{i-j-1}^{x+1} \times \mu_{i-j}^{x+1} \nu_{i-j}^{x+1} \varphi^{q-i+j,i-j} \times \hat{\mu}_{i-j+1} \times \]
\[ \cdots \times \hat{\mu}_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi. \]
In the $i-j$ coordinate, we have the character $\mu_{i-j}^j \varphi_i^{q^j i^j - j}$. By Lemma 8.5, we know that going through all possible choices of $\gamma$, $\varphi_i^{q^j i^j - j}$ runs through all characters in $\text{Irr}(B_{i-j}/B_{i-j})$. Recall $D_{i-j,q} = \{1 + \beta x^{i-j} \mid \beta \in [F, \sigma]\}$. We know that $B_{i-j} = B_{i-j,q} \hat{+} D_{i-j,q}$. Thus, $\text{Irr}(B_{i-j}) = \text{Irr}(B_{i-j}/B_{i-j,q}) \times \text{Irr}(B_{i-j}/D_{i-j,q})$, and hence, the coset $\mu_{i-j}^j \text{Irr}(B_{i-j}/B_{i-j,q})$ contains a unique character $\mu_{i-j}^* \in \text{Irr}(B_{i-j}/D_{i-j,q})$.

Fix $\gamma \in F$ so that $\mu_{i-j}^j \varphi_i^{q^j i^j - j} = \mu_{i-j}^j$. Notice that this fixes $s_1$. For $l = \frac{q+1}{2}, \ldots, i-j-1$, set $\mu_l^j = \mu_{i-j}^j \nu_l$ so that

$$
(\theta_j)^{s_1^{-1}} = \mu_{\frac{q+1}{2}} \times \cdots \times \mu_{i-j-1} \times \mu_{i-j} \times \mu_{i-j+1} \times \cdots \times \mu_1 1_{B_{i-1}} \times \cdots \times 1_{B_{q-1}} \times \varphi.
$$

Let $s_2 = 1 + \delta x^j$ where $\delta$ is any element in $F_q$. As before, we mention that we will fix $\delta$ later. By Lemma 10.5, we have

$$
(\theta_j^{s_1^{-1}})^{s_2^{-1}} = \theta_j^{s_1^{-1}} \times (\kappa_{\frac{q+1}{2}} \times \cdots \times \kappa_{i-j-1} \times (\hat{\mu}_i)^{j-i-j} \times 1_{B_{i-j+1}} \times \cdots \times 1_{p_q}).
$$

We see that the $i-j$ coordinate of $(\theta_j^{s_1^{-1}})^{s_2^{-1}}$ will contain the character $\mu_{i-j}^*(\hat{\mu}_i)^{j-i-j}$.

We know $\text{ker}(\hat{\mu}_i) = \{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\}$, and by Lemma 4.10, we see that $\text{ker}(\hat{\mu}_i) = \{1 + \beta x^i \mid \beta \in \langle \alpha^b, F \rangle_{1,i-1}\}$ where $b \equiv (\frac{p-1}{p^j-1})(\text{mod } o(\alpha))$. Let $c \equiv (\frac{p^j-1}{p-1})(\text{mod } o(\alpha))$ and $E = \{1 + \beta x^{i-j} \mid \beta \in \alpha^c \mathbb{Z}_p + [F, \sigma]\}$. By Lemma 10.2, we know that as $\delta$ runs over $F_q$, $(\hat{\mu}_i)^{j-i-j}$ runs through the set $\text{Irr}(B_{i-j}/E)$. By Lemma 10.3, we know that $F_q = \alpha^c \mathbb{Z}_p + \langle \alpha, F_q \rangle_{1,i-j-1}$. Let $E' = \{1 + \beta x^{i-j} \mid \beta \in \langle \alpha, F_q \rangle_{1,i-j-1}\}$. We see that $B_{i-j} = E + E'$ and $E \cap E' = D_{i-j,q}$, so $B_{i-j} = B_{i-j,q} = E/D_{i-j,q} \hat{+} E'/D_{i-j,q}$. Hence, we have $\text{Irr}(B_{i-j}/D_{i-j,q}) = \text{Irr}(B_{i-j}/E) \times \text{Irr}(B_{i-j}/E')$, and thus, the coset $\mu_{i-j}^* \text{Irr}(B_{i-j}/E)$ has a unique character $\hat{\mu}_{i-j} \in \text{Irr}(B_{i-j}/E')$. Notice that $\hat{\mu}_{i-j}$ has the property needed in the conclusion.
Fix $\delta \in F_q$ so that $\mu_{i-j}^*(\hat{\mu}_i)^{j,i-j}_\delta = \hat{\mu}_{i-j}$. It now follows that

$$\theta_j^{(s_2s_1)} = \mu_{q+1}^j \times \cdots \times \hat{\mu}_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi,$$

as desired. \hspace{1cm} q.e.d.

We now have enough results to determine the location of the stabilizer of these types of characters within our group.

Lemma 10.7 Fix $j \in \mathbb{Z}^+$ so that $\frac{q+3}{2} \leq j \leq q-1$ and fix $\alpha \in F_q$. Let

$$\theta = \mu_{\frac{q+3}{2}} \times \cdots \times \mu_j \times 1_{B_{j+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi$$

such that $\{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\} \subseteq \ker(\mu_i)$ for $i = 1, \ldots, j-1$ and $\ker(\mu_j) = \{1 + \beta x^j \mid \beta \in \langle \alpha, F \rangle_{1,j-1}\}$. Then the stabilizer of $\theta$ in $P$ is contained in $QP^{\frac{q+1}{2}}$.

Proof. Label $S$ as the stabilizer of $\theta$ in $P$. Suppose $s = 1 + \alpha_1 x + \cdots + \alpha_q x^q \in S$. Then we know that for all $t \in P^{\frac{q+3}{2}}$, $\theta(t) = \theta^{s^{-1}}(t) = \theta(t) \theta([t,s])$. Thus, we have $\theta([t,s]) = 1$ for all $t \in P^{\frac{q+3}{2}}$. Applying Lemma 5.1 to $[t,s]$ we see that

$$\theta([t,s]) = \mu_{\frac{q+3}{2}}(1 + \delta_1 x^{\frac{q+3}{2}}) \cdots \mu_j(1 + \delta_{j-\frac{q+1}{2}} x^j) \varphi(1 + \delta_{q-1} x^q).$$

By Lemma 5.2, $\delta_k = \sum_{i=1}^{k} \langle \alpha_i, d_{k-i+1} \rangle_{i,k-i}$. Using this result, we can replace each $\delta_i$ and obtain

$$\theta([t,s]) = \mu_{\frac{q+3}{2}}(1 + \langle \alpha_1, d_1 \rangle_{1,\frac{q+3}{2}} x^{\frac{q+3}{2}}) \cdots \mu_j(1 + \sum_{i=1}^{j-\frac{q+1}{2}} \langle \alpha_i, d_{j-\frac{q+1}{2}} \rangle_{i,j-i} x^j) \varphi(1 + \sum_{i=1}^{q-1} \langle \alpha_i, d_{\frac{q+1}{2}-i} \rangle_{i,q-i} x^q).$$
Notice that since $\beta_{q+1}, \ldots, \beta_{q-1}$ are independent of each other, $d_1, \ldots, d_{q-1}$ are also independent. Because of this, we can choose $l$ so that $d_{l+1} \neq 0$ and $d_k = 0$ for $k \neq l+1$.

This implies $\delta_j = 0$ if $j < l + 1$ and $\delta_j = (\alpha_{j-l}, d_{l+1})_{j-l,l}$, otherwise. Similarly, for $j - \frac{q-1}{2} \leq l \leq \frac{q-3}{2}$, we have

$$\varphi(1 + \langle \alpha_{\frac{q-1}{2}-l}, d_{l+1} \rangle_{q-l,l}, x^q) = (\varphi)_{\alpha_{\frac{q-1}{2}-l}}(1 + d_{l+1}x^r) = 1,$$

for all $d_{l+1} \in F$. By Lemma 8.5, this implies $\alpha_{\frac{q-1}{2}-l} \in F_q$. Notice that $\frac{q-1}{2} - (j - \frac{q-1}{2}) = q - j - 1$. Thus, we have $\alpha_1, \alpha_2, \ldots, \alpha_{q-j-1} \in F_q$.

For $1 \leq l \leq j - \frac{q-3}{2}$, we actually show a stronger result. For each $l$, in addition to showing that $\alpha_{\frac{q-1}{2}-l} \in F_q$, we show that $\alpha_l \in \alpha_{\frac{q-1}{2}-1}Z_p$, where $l' = j - \frac{q-1}{2} - l$. We will do this by induction on $l'$.

When $l' = 1$, we have $l = j - \frac{q-1}{2} - 1 = j - \frac{q-3}{2}$ and $l^* = j - \frac{q-3}{2} - 1 + \frac{q-1}{2} = j - 1$.

The equation to consider here is

$$\mu_j(1 + \langle \alpha_1, d_{l+1} \rangle_{l,l}, x^j) \varphi(1 + \langle \alpha_{\frac{q-1}{2}-l}, d_{l+1} \rangle_{\frac{q-1}{2}-l,l}, x^q)$$

$$= (\mu_j)_{\alpha_1}^{l+1-j}(1 + d_{l+1}x^r) \cdot (\varphi)_{\alpha_{\frac{q-1}{2}-l}}(1 + d_{l+1}x^r) = 1,$$

for all $d_{l+1} \in F$. By Lemma 8.5, we know that $B_{j,q} \subseteq \ker((\varphi)_{\alpha_{\frac{q-1}{2}-l}}(1 + d_{l+1}x^r))$. From our equation above, this implies $B_{j,q} \subseteq \ker((\mu_j)_{\alpha_1}^{l+1-j})$. On the other hand, we have seen that $\alpha_1 \in F_q$, so we may use Lemma 10.2 to see that $D_{j,q} \subseteq \ker((\mu_j)_{\alpha_1}^{l+1-j})$. Since $B_j = B_{j,q} + D_{j,q}$, we deduce that $(\mu_j)_{\alpha_1}^{l+1-j}(1 + d_{l+1}x^r) = 1$. By Lemma 10.2, this implies that $\alpha_1 \in \alpha Z_p$.

This gives us $(\varphi)_{\alpha_{\frac{q-1}{2}-l}}(1 + d_{l+1}x^r) = 1$. By Lemma 8.5, we obtain $\alpha_{\frac{q-1}{2}-l} \in F_q$.

Note that $\frac{q-1}{2} - l = \frac{q-1}{2} - (j - \frac{q-1}{2} - 1) = q - j$, so we have $\alpha_{q-j} \in F_q$. 
We now come to the inductive step and assume that \( l' > 1 \), and that the result holds for \( 1, \ldots, l' - 1 \). In other words, we have \( \alpha_1, \ldots, \alpha_{q+j+l'-1} \in F_q \) and \( \alpha_i \in \alpha_{\frac{q-1}{2} - l} \mathbb{Z}_p \) for \( i = 1, \ldots, l' - 1 \). We obtain the equation

\[
\prod_{i=1}^{l'} \mu_{l'+i}(1 + \langle \alpha_i, d_{l'+i-1}, x^{l'+i} \rangle) \varphi(1 + \langle \alpha_{l'+i-1}, d_{l'+i} \rangle x^{l'+i})
\]

\[
= \prod_{i=1}^{l'} (\mu_{l'+i})_{\alpha_i} (1 + d_{l'+i} x^{l'+i}) \cdot (\varphi)^{\frac{q-1}{2} - l}_{\alpha_{\frac{q-1}{2} - l}} (1 + d_{l'+i} x^{l'+i}) = 1,
\]

for all \( d_{l'+i} \in F \).

For \( i = 1, \ldots, l' - 1 \), we know that \( \ker(\mu_{l'+i}) \) contains

\[
\{ 1 + \beta x^{l'+i} \mid \beta \in \langle \alpha, F \rangle_{1,l'+i-1} \} = \{ 1 + \beta x^{l'+i} \mid \beta \in \langle \alpha_{\frac{q-1}{2} - l}, F \rangle_{i,l'+i-1} \},
\]

where equality comes from applying Lemma 4.10. Since \( \alpha_i \in \alpha_{\frac{q-1}{2} - l} \mathbb{Z}_p \), this implies

\[
(\mu_{l'-i})_{\alpha_i} (1 + d_{l'+i} x^{l'}) = 1 \text{ for } i = 1, \ldots, l' - 1.
\]

Thus, our equation becomes

\[
(\mu_j)_{\alpha_{l'}} (1 + d_{l'+i} x^{l'}) \cdot (\varphi)^{\frac{q-1}{2} - l}_{\alpha_{\frac{q-1}{2} - l}} (1 + d_{l'+i} x^{l'}) = 1.
\]

By Lemma 8.5, we know that \( B_{l'+1,q} \subseteq \ker((\varphi)^{\frac{q-1}{2} - l}_{\alpha_{\frac{q-1}{2} - l}}) \), and so, \( B_{l'+1,q} \subseteq \ker((\mu_j)_{\alpha_{l'}}) \).

On the other hand, from Lemma 10.2, we have \( D_{l'+1,q} \subseteq \ker((\mu_j)_{\alpha_{l'}}) \). This implies

\[
(\mu_j)_{\alpha_{l'}} (1 + d_{l'+i} x^{l'}) = 1, \text{ and hence, } \alpha_{l'} \in \alpha_{\frac{q}{2} - 1} \mathbb{Z}_p \text{ by Lemma 10.2 since}
\]

\[
\ker(\mu_j) = \{ 1 + \beta x^l \mid \beta \in \langle \alpha, F \rangle_{1,l-1} \} = \{ 1 + \beta x^l \mid \beta \in \langle \alpha_{\frac{q}{2} - 1} \mathbb{Z}_p, F \rangle_{l,l'} \}
\]

by Lemma 4.10. Finally, we obtain \( (\varphi)^{\frac{q-1}{2} - l}_{\alpha_{\frac{q-1}{2} - l}} (1 + d_{l'+i} x^{l'}) = 1 \), and by Lemma 8.5, this implies \( \alpha_{\frac{q-1}{2} - l} \in F_q \). This proves the inductive step and that for \( s \) to stabilize \( \theta \),
s must be in $QP^{q+1}_2$. Therefore, $S \subseteq QP^{q+1}_2$. \[ q.e.d. \]

In general, we define $A_i$ for $i = \frac{q+1}{2}, \frac{q+3}{2}, \ldots, q - 1$ to be the set of all characters in $\text{Irr}(P^{q+1}_2)$ that are $P$-conjugate to some character of the form $\theta = \mu_1 \times \cdots \times \mu_i \times 1_{B_i} \times \cdots \times 1_{B_{q-1}} \times \varphi$, where $\mu_j \in \text{Irr}(B_j)$ for $j = \frac{q+1}{2}, \ldots, i$ and $\ker(\mu_i) = \{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\}$, for some $\alpha \in F_q$. Recall Lemma 4.7 tells us that $\langle \alpha, F \rangle_{1,i-1}$ is a hyperplane in $F$. Since $\frac{p^r-1}{p-1}$ is relatively prime to $\frac{p^q-1}{p-1}$, raising to the $\frac{p^r-1}{p-1}$ power is a bijection for the cyclic group of order $\frac{p^q-1}{p-1}$. Hence, there is an element $\beta \in F$ so that $\beta^{\frac{p^q-1}{p-1}} = \alpha$. Therefore, $\langle \beta, F \rangle_{1,i-1} = \alpha \ker(Tr)$. As a result, the particular elements $\alpha \in F$ for which $\ker(\mu_i) = \{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\}$ are independent of $i$. Notice that the definition of $A_{\frac{q+1}{2}}$ here is consistent with the previous definition of $A_{\frac{q+1}{2}}$.

**Lemma 10.8** Every character in $\text{Irr}(P^{q+1}_2 \mid \varphi)$ lies in some $A_j$ for $j = \frac{q-1}{2}, \ldots, q - 1$.

**Proof.** Suppose $\theta \in \text{Irr}(P^{q+1}_2 \mid \varphi)$, then

$$\theta = \mu_{\frac{q+1}{2}} \times \cdots \times \mu_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi,$$

where $\mu_i \neq 1$. We say that $i$ is the length of $\theta$. We prove the lemma by induction on $i$. First suppose all coordinates of $\theta$ other than $\varphi$ are 1. In this case, we have $\theta \in A_{\frac{q+1}{2}}$ by definition of $A_{\frac{q+1}{2}}$, and we say that $\theta$ has length $\frac{q-1}{2}$. We now fix $i \geq \frac{q+1}{2}$, and we assume the result holds for all characters $\theta$ with length at most $i - 1$. Let $s = 1 + \gamma x^{q-i}$, and by Lemma 10.4, we have

$$\theta^{s-1} = \theta \cdot (\nu_{\frac{q+1}{2}} \times \cdots \times \nu_{i-1} \times \varphi^{q-i,i} \times 1_{B_{i+1}} \times \cdots \times 1_{P_0}).$$

In the $i$th coordinate, we have $\mu_i \varphi^{q-i,i}$. We know from Lemma 8.5 that as $\gamma$ runs through $F$, then $\varphi^{q-i,i}$ will run over all characters in $\text{Irr}(B_i/B_{i+1})$. We have seen
that $\text{Irr}(B_i) = \text{Irr}(B_i/B_{i,q}) \times \text{Irr}(B_i/D_{i,q})$. Thus the coset $\mu_i\text{Irr}(B_i/B_{i,q})$ has a unique character $\mu_i^* \in \text{Irr}(B_i/D_{i,q})$. We choose $\gamma \in F$ so that $\mu_i^* \varphi_{\gamma}^{-i} = \mu_i^*$. Observe that

$$\theta^{*^{-1}} = \mu_i^{l+1} \times \cdots \times \mu_i^{l+1} \times \mu_i^* \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi.$$ 

If $\mu_i^* = 1$, then $\theta^{*^{-1}}$ has length at most $(i - 1) - \frac{q+1}{2}$, and so, by the inductive hypothesis, $\theta^{*^{-1}}$ lies in one of $A_{q+1}, \ldots, A_{i-1}$, and we are done in this case. Thus, $\mu_i^* \neq 1$. We know that $D_{i,q} \subseteq \ker(\mu_i^*)$. Now, $\ker(\mu_i^*) \cap B_{i,q}$ is a hyperplane in $B_{i,q}$. It follows that $\ker(\mu_i^*) \cap B_{i,q} = \{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\}$, and by Lemma 10.1, we have $\ker(\mu_i^*) = \{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\}$. This implies $\mu_i^* \in A_i$, and proves the result.

q.e.d.

Lemma 10.9 For $A_i$ defined as above,

$$\text{cd}(G \mid A_i) = \left\{ p^{\left(\frac{q+1}{2}\right)\left(qr-q+1\right)} \left( p^r - 1 \right) \right\}.$$ 

Proof. Let $\theta \in A_i$ for some $i$. By definition of $A_i$, we can assume that $\theta$ is conjugate to a character of the form

$$\gamma = \mu_{i+1} \times \cdots \times \mu_i \times 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi,$$

where $\ker(\mu_i) = \{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\}$. By Lemma 10.6, we may assume that $\{1 + \beta x^i \mid \beta \in \langle \alpha, F \rangle_{1,i-1}\} \subseteq \ker(\mu_i)$ for $l = \frac{q+1}{2}, \ldots, i - 1$. By Lemma 10.7, we know that the stabilizer of $\gamma$ is contained in $QP^{\frac{q+1}{2}}$. Again, we define $Q^i = P^j \cap Q$. Now, $Q^i \cap B_l = B_{l,q} \cong B_l/D_{l,q} \cong F_q$ for $l = \frac{q+1}{2}, \ldots, i$. We also know $Q \cap B_l = B_{l,q}$, and hence, we have

$$\frac{P^{\frac{q+1}{2}}}{P^{i+1}} = \frac{B_{\frac{q+1}{2},q} + P^{i+1}}{P^{i+1}} + \frac{D_{\frac{q+1}{2},q} + P^{i+1}}{P^{i+1}}.$$
Using a similar argument to that of Lemma 9.1 we obtain \(QP^{\frac{q+1}{r}}/(D_{\frac{q+1}{r}}q^i P^{i+1}) \cong Q/Q^{i+1}\). With this in mind, we can view \(\gamma\) as a non-principal character of \(\text{Irr}(QP^{\frac{q+1}{r}}/Q^{i+1})\) by restricting \(\gamma\) to \(Q^{\frac{q+1}{r}}\). Notice that \(\gamma_{Q^{i+1}} = 1_{B_{i+1}} \times \cdots \times 1_{B_{q-1}} \times \varphi\) and \(\mu_{\frac{q+1}{r}} \times \cdots \times \mu_i \times 1_{B_{q+1}} \times \cdots \times 1_{P_1}\). By Lemma 8.2, \(\gamma_{Q^{i+1}}\) extends to \(QP^{\frac{q+1}{r}}\). By Gallagher’s theorem, the characters in \(\text{Irr}(QP^{\frac{q+1}{r}} | \gamma_{Q^{i+1}})\) are in bijection with characters in \(\text{Irr}(Q/Q^{i+1})\).

Since \(\mu_i \neq 1\), the characters in \(\text{Irr}(QP^{\frac{q+1}{r}} | \gamma)\) are in bijection with characters in \(\text{Irr}(Q/Q^{i+1} | Q^{i}/Q^{i+1})\). Using Theorem 4.4 from [16], we have that characters in \(\text{Irr}(Q/Q^{i+1} | Q^{i}/Q^{i+1})\) all have degree \(p^{\left(\frac{q+1}{r}\right)\left(i-1\right)}\). Thus, characters in \(\text{Irr}(QP^{\frac{q+1}{r}} | \gamma)\) will all have degree \(p^{\left(\frac{q+1}{r}\right)\left(i-1\right)}\). Using Clifford theory, these induce irreducibly to \(P\) of degree \(p^{\left(\frac{q+1}{r}\right)\left(qr-q+i-1\right)}\). Under the action of \(C\), these characters are permuted in orbits of size \(\frac{p^{qr-1}}{p-1}\) and hence, induce irreducibly to \(CP\). Thus, for \(\text{Irr}(CP | A_i)\), the character degree is \(p^{\left(\frac{q+1}{r}\right)\left(qr-q+i-1\right)}\left(\frac{p^{qr-1}}{p-1}\right)\). Since \(G\) stabilizes these characters, we have

\[
\text{cd}(G | A_i) = \left\{ p^{\left(\frac{q+1}{r}\right)\left(qr-q+i-1\right)}\left(\frac{p^{qr-1}}{p-1}\right) \right\}.
\]

q.e.d.

**Theorem 10.10** Set

\[
A^* = \left\{ p^{\left(\frac{q+1}{r}\right)\left(qr-q+i-1\right)}\left(\frac{p^{qr-1}}{p-1}\right) \mid i = 0, 1, \ldots, q-1 \right\} \text{ and }
\]

\[
B^* = \left\{ \left(\frac{p^{qr-1}}{p-1}\right)^i\left(\frac{p^{qr-1}}{p-1}\right) \mid i = 0, 1, \ldots, q-2 \right\}.
\]

Then the set of all character degrees of the group \(G\) is given by

\[
\text{cd}(G) = \left\{ 1, q, r, qr, qP^{\frac{q+1}{r}}qr^i, \left(\frac{p^{qr-1}}{p-1}\right), \left(\frac{p^{qr-1}}{p^{qr-1}}\right) \right\}.
\]
\[
qp^{(\frac{q-1}{2})(qr-q)} \left( \frac{p^{qr} - 1}{p^q - 1} \right) \} \cup A^* \cup B^*.
\]

**Proof.** As was discussed in Chapter 6, we know that \( \text{cd}(G) = \text{cd}(G/P^q) \cup \text{cd}(G/P^q) \). From Lemma 6.2, we have that
\[
\text{cd}(G/P^q) = \left\{ 1, q, r, qr, \left( p^{qr} - 1 \right) \left( p^q - 1 \right)^i \right\} \mid i = 0, 1, \ldots, q - 2 \} = \{1, q, r, qr\} \cup B^*.
\]
Recall \( A \) was defined to be the characters \( \varphi \in \text{Irr}(P^q) \) whose kernels correspond to \( \langle \alpha, F \rangle_{i,q-i} \) for some \( \alpha \in F \) and \( 1 \leq i \leq \frac{q-1}{2} \), and \( B \) was defined to be the characters \( \varphi \in \text{Irr}(P^q) \) whose kernels do not correspond to \( \langle \alpha, F \rangle_{i,q-i} \) for all \( \alpha \in F \) and \( 1 \leq i \leq \frac{q-1}{2} \).

Now, the remaining characters of \( G \) are in \( \text{Irr}(G/P^q) \), which are in \( \text{Irr}(G/B) \cup \text{Irr}(G/A) \). To see this, consider \( \chi \in \text{Irr}(G/P^q) \), and let \( \varphi \) be an irreducible constituent of \( \chi_{P^q} \). Since \( \chi \in \text{Irr}(G/P^q) \), we know that \( \varphi \neq 1 \). Since \( P^q \) is an elementary abelian \( p \)-group, the kernel of \( \varphi \) will be a hyperplane in \( P^q \). By Corollary 4.8, we know that some of the hyperplanes in \( P^q \) have the form \( \langle a, F \rangle_{i,q-i} \) for some \( a \in F \), and the rest do not. If \( \ker(\varphi) \) does not have the form \( \langle a, F \rangle_{i,q-i} \) for any \( a \in F \), then \( \varphi \in B \). If \( \ker(\varphi) = \langle a, F \rangle_{i,q-i} \) for some \( a \in F \), then \( \varphi \in A \). This implies \( \text{Irr}(G/P^q) \subseteq \text{Irr}(G/B) \cup \text{Irr}(G/A) \). The other containment is trivial, so we have \( \text{Irr}(G/P^q) = \text{Irr}(G/B) \cup \text{Irr}(G/A) \).

Lemma 7.3 tells us that the set of character degrees whose kernels do not correspond to hyperplanes is given by
\[
\text{cd}(G/B) = \left\{ qp^{\frac{q-1}{2}qr} \left( p^{qr} - 1 \right) \left( p^q - 1 \right) \} \right\}.
\]
The characters of $G$ whose kernels correspond to hyperplanes are found in Lemmas 8.3 and 10.9. From this we have $\text{cd}(G | \mathcal{A}_i)$ is the set

$$\left\{ p^{(\frac{q - 1}{2})}(q - 2)(\frac{p^{qr} - 1}{p^q - 1}), qp^{(\frac{q - 1}{2})}(\frac{p^{qr} - 1}{p^q - 1}), p^{(\frac{q - 1}{2})(q - 4 + i)}(\frac{p^{qr} - 1}{p^q - 1}) \right\} \cap \mathcal{A}_i = 0, 1, \ldots, q - 3$$

Combining all of these degrees we have

$$\text{cd}(G) = \text{cd}(G/P^q) \cup \text{cd}(G/\mathcal{B}) \cup \text{cd}(G | \mathcal{A}_i),$$

where $i = \frac{q + 1}{2}, \ldots, q - 1$, as desired. 

\textit{q.e.d.}

Clearly, $p, q,$ and $r$ are all vertices in $\rho(G)$. To determine the remaining vertices in $\rho(G)$, we need to find the sets of prime divisors of $\frac{p^{qr} - 1}{p^q - 1}$ and $\frac{p^{qr} - 1}{p^r - 1}$. The easiest way of doing this is in terms of cyclotomic polynomials. Recall from Chapter 3, we chose our primes $p, q,$ and $r$ so that $\Phi_q(p), \Phi_r(p),$ and $\Phi_{qr}(p)$ are pairwise relatively prime. We also remind the reader that because $q$ and $r$ are primes, $\Phi_q(p) = \frac{p^q - 1}{p - 1}$ and $\Phi_r(p) = \frac{p^r - 1}{p - 1}$.

First, consider $\frac{p^{qr} - 1}{p^q - 1}$. Recall from the discussion in Chapter 3, we can write

$$p^{qr} - 1 = \Phi_1(p)\Phi_q(p)\Phi_r(p)\Phi_{qr}(p).$$

Hence, $\frac{p^{qr} - 1}{p^q - 1} = \Phi_q(p)\Phi_r(p)\Phi_{qr}(p)$. Similarly,

$$\frac{p^{qr} - 1}{p^r - 1} = \frac{\Phi_1(p)\Phi_q(p)\Phi_r(p)\Phi_{qr}(p)}{\Phi_1(p)\Phi_q(p)} = \Phi_r(p)\Phi_{qr}(p).$$
Thus, we need to consider these two products and the primes that divide them. By the choices of $p, q,$ and $r$ for our group, we know $\Phi_q(p), \Phi_r(p),$ and $\Phi_{qr}(p)$ will be distinct sets of primes in $\rho(G)$. For our purposes we will label $\Phi_n$ to be the set of all primes that divide $\Phi_n(p)$. Using this notation, we see that we have the sets $\Phi_q, \Phi_r,$ and $\Phi_{qr}$ that will be part of the graph.

Referring to the degrees in Theorem 10.10, notice that primes in $\Phi_q, \Phi_r,$ and $\Phi_{qr}$ are all incident to each other and to $p$. Also notice that $r$ is only adjacent to $q$.

It should also be mentioned that relative to the character degree graph, each set, $\Phi_n$, will form a complete graph $\Delta(G)$ and will not affect the diameter. Thus, we treat these sets of primes on the graph as single vertices.

**Theorem 10.11** The set of vertices of $\Delta(G)$ is

$$\rho(G) = \{p, q, r\} \cup \Phi_q \cup \Phi_r \cup \Phi_{qr}.$$  

The character degree graph is given by the graph in Figure 10.1.

![Figure 10.1: The character degree graph of $G$](image_url)

As is clearly seen in Figure 10.1, $\Delta(G)$ is isomorphic to the graph given by Lewis and thus, has diameter three. We see from the graph that the diameter is being
determined in this case by the number of edges in a path between \( r \) and \( \Phi_q \). We mentioned in the beginning that fixing \( p = 2, q = 3 \), and choosing a general \( r \) appropriately would not change the argument given by Lewis. We gain insight from the graph as to why this is so.

Are there other groups whose degree graphs are the graph in Figure 10.1? If so, do those groups have the same structure as the family of groups constructed here? The answers to these questions are not known, as of yet.
BIBLIOGRAPHY


