ON THE GROUP CLASS EQUATION
ON THE GROUP CLASS EQUATION

by

John Poland, M.Sc.

A thesis submitted to the Faculty of Graduate Studies
and Research in partial fulfilment of the requirements for
the degree of Doctor of Philosophy.

Department of Mathematics,
McGill University,
Montreal.

March 1966.
PREFACE

I would like to express my gratitude to my director of research, Professor H. Schwerdtfeger, for the suggestion of this topic and his encouragement during the execution of this thesis.
# TABLE OF CONTENTS

**On the Group Class Equation**

<table>
<thead>
<tr>
<th>Chapter One: Introduction.</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1: Landau's Theorem</td>
<td></td>
</tr>
<tr>
<td>1.2: Notation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter Two: On Burnside's Note A.</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1: Introduction</td>
<td>14</td>
</tr>
<tr>
<td>2.2: Conditions upon the group class equation</td>
<td>16</td>
</tr>
<tr>
<td>2.3: A list of groups with $k(G) \leq 7$</td>
<td>61</td>
</tr>
<tr>
<td>2.4: Proof</td>
<td>65</td>
</tr>
<tr>
<td>2.5: Conjectures</td>
<td>85</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter Three: Groups Of Prime Power Order.</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1: The Duality Principle</td>
<td>87</td>
</tr>
<tr>
<td>3.2: $p$-Groups with minimum class number</td>
<td>91</td>
</tr>
<tr>
<td>3.3: The least upper bound for $2$-groups</td>
<td>99</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter Four: Other Authors.</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>118</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>121</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bibliography</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>123</td>
</tr>
</tbody>
</table>
Section 1.1: Landau's Theorem.

Each finite group $G$ of elements $l, x, y, \ldots$ can be partitioned into non-intersecting sets of elements which are conjugate if and only if they belong to the same set. These sets are called the conjugate classes of $G$, or simply the classes of $G$. If we denote the order of $G$ by $g$, the number of these classes by $k$, and the classes themselves by $K_1, K_2, \ldots, K_k$, then we have $x, y \in K_i$ iff there is some $z \in G$ so $x = y z y^{-1}$, $K_i \cap K_j$ is empty if $i \neq j$, and

\[(1.1.1) \quad G = K_1 + K_2 + \cdots + K_k.\]

This latter expression of $G$ as a disjoint union of its classes we shall call the group class equation; it is the subject of this thesis.

By denoting the number of elements in $K_i$ by $h_i$, the group class equation yields

\[(1.1.2) \quad g = h_1 + h_2 + \cdots + h_k.\]
The most important condition on (1.1.2) is that each $h_i$ must divide $g$. In fact, the following theorem is well known (see Burnside [7], p.31).

(1.1.3) Theorem: For each element $x$ of $K_i$, the elements of $G$ which commute with $x$ form a group, the centralizer $C_G(x)$ of $x$ over $G$, of order $m_i = g/h_i$.

Hence $1/m_i = h_i/g$ and if we divide by $g$ in (1.1.2),

$$\frac{1}{m_1} + \frac{1}{m_2} + \cdots + \frac{1}{m_k} = 1.$$ 

It is this equation in which we will be the most interested. Because we can derive any one of the equations (1.1.1), (1.1.2), and (1.1.4) from another, we will use the term "group class equation" for all of them.

We impose the condition that the $m_i$ (and $h_i$) are numbered such that $m_1 \geq m_2 \geq \cdots \geq m_k$, or $h_1 \leq h_2 \leq \cdots \leq h_k$.

Since $1 \not\in G$ implies $G \ngtr C_G(x) \ngtr \langle x \rangle \neq 1$, where $\langle x \rangle$ is the cyclic group generated by $x$, then for each $i$, $g \geq m_i \geq 2$, including the case of the unity element of $G$, for which we take the first class $K_1 = 1$, $h_1 = 1$, and $m_1 = g$. Therefore

$$g = m_1 \geq m_2 \geq \cdots \geq m_k \geq 1.$$ 

From these elementary properties of the group class equation, we can deduce an interesting existence theorem, discovered by E. Landau ([22]) in 1903.
(1.1.6) **Theorem:** There are only finitely many non-isomorphic finite groups having a given number $k$ of classes of conjugate elements.

**Proof:** It is well known that there are only finitely many non-isomorphic groups $G$ of given order $g$. In fact, a group $G$ is completely defined (up to isomorphism) by its $g \times g$ multiplication table (Burnside [7], p.20) and since there are at most $g$ possibilities - the $g$ elements of $G$ - for each place in the table, the number of tables, and hence groups of order $g$, is bounded by $g^{g \times g} = g^g$.

The theorem is proved if we can show that for every given $k$ there is a finite number $f(k)$ such that the order $g$ of any group $G$ with $k$ conjugate classes must be smaller than $f(k)$. Indeed, by the above remark, the number of groups of order less than the given finite number $f(k)$ is finite, and the groups with $k$ classes must be distributed amongst them.

In order to find a value for $f(k)$ which will suffice, we consider the group class equation (1.1.4), with $m_1 = g$ as noted in (1.1.5). Solving (1.1.4) for $m_1$, we have

\[
g = \left[1 - \left(\frac{1}{m_k} + \frac{1}{m_{k-1}} + \cdots + \frac{1}{m_2}\right)\right]^{-1};
\]

if we maximize the possible value of the expression on the right hand side of this equality, keeping $k$ fixed, we can take this value for $f(k)$. To do this, of course, we must
choose the minimum possible values of \( m_k, m_{k-1}, \ldots, m_2 \).

Since \( m_k \geq 2 \), take \( m_k = 2 \). Then \( m_{k-1} \geq m_k = 2 \), and \( m_{k-1} = 2 \) in (1.1.4) means \( k = 2 \) and \( g = 2 \). For \( k > 2 \), take \( m_{k-1} = 3 \).

Similarly \( k = 3 \) if and only if \( \frac{1}{m_{k-2}} = 1 - \left( \frac{1}{2} + \frac{1}{3} \right) = \frac{1}{6} \), while otherwise the minimum possible value of \( m_{k-2} \) is 7.

We wish to continue in this manner.

It is simple to prove by induction on \( n \) that if

\[ 1 \leq n \leq k-2, \text{ and if we take } m_k = 2 \text{ and } m_{k-1} = m_k \cdot m_{k-1} \ldots m_{k-i+1} + 1 \text{ for } 1 \leq i < n, \text{ then } 1 - \left( \frac{1}{m_k} + \cdots + \frac{1}{m_{k-n+1}} \right) = \frac{1}{m_{k-n+1}}. \]

Indeed, \( 1 - (1/m_k) = 1 - 1/2 = 1/2 = 1/m_k \); now suppose it is true for any positive integer \( n' < n \).

Then

\[ 1 - \left( \frac{1}{m_k} + \cdots + \frac{1}{m_{k-n+1}} \right) = \left[ 1 - \left( \frac{1}{m_k} + \cdots + \frac{1}{m_{k-n+2}} \right) \right] - \frac{1}{m_{k-n+1}} \]

\[ = \frac{1}{m_k \cdots m_{k-n+2}} - \frac{1}{m_{k-n+1}} \]

by induction. But \( m_{k-n+1} = m_k \cdots m_{k-n+2} + 1 \) and hence the expression reduces to

\[ \frac{(m_k \cdots m_{k-n+2} + 1) - (m_k \cdots m_{k-n+2})}{(m_k \cdots m_{k-n+2})(m_{k-n+1})} = \frac{1}{m_k \cdots m_{k-n+1}} \]

as was to be shown.

But if \( 1 \leq n \leq k-2 \) and if \( m_k = 2 \) and \( m_{k-1} = m_k \cdot m_{k-1} \cdots m_{k-i+1} + 1 \) for \( 1 \leq i < n \), then \( m_{k-n} > m_k \cdots m_{k-n+1} \) since

\[ \frac{1}{m_k-n} < \frac{1}{m_1} + \frac{1}{m_2} + \cdots + \frac{1}{m_{k-n}} = 1 - \left( \frac{1}{m_k} + \cdots + \frac{1}{m_{k-n+1}} \right) = \frac{1}{m_k \cdots m_{k-n+1}} \]
as shown above. We conclude that for the minimum possible values of \( m_k, m_{k-1}, \ldots, m_2 \) we must take \( m_k = 2 \) and \( m_{k-n} = m_k \cdot m_{k-1} \cdots m_{k-n+1} + 1 \) \((1 \leq n \leq k-2)\). With this choice of values, we have \( m_1 = m_k \cdot m_{k-1} \cdots m_2 \) by (1.1.7). But \( g = m_1 \). Therefore the maximum possible value of the order \( g \) of a group with \( k \) classes, or \( f(k) \), is \( m_k \cdot m_{k-1} \cdots m_3 \cdot m_2 \) where \( m_k = 2 \) and \( m_{k-i} = m_k \cdot m_{k-i+1} + 1 \) \(\text{for} \ 1 \leq i \leq k-2 \).

With the existence of \( f(k) \), our proof is complete.

Q.E.D.

In the original proof, in [22], Landau did not calculate \( f(k) \), but used induction to show that if \( m_{k-j} \) was bounded for \( j < i \) then \( m_{k-i} \) was bounded and hence by (1.1.6) \( g \) was bounded too.

(1.1.8) Corollary: If a finite group \( G \) of order \( g \) has \( k \) conjugate classes, then \( g < 3^{2^k-2} \).

Proof: We have shown in (1.1.6) that \( g < f(k) \) where

\[
f(k) = m_k \cdot m_{k-1} \cdots m_2 \quad \text{and} \quad m_k = 2, \ m_{k-1} = m_k \cdots m_{k-i+1} + 1 \quad \text{for} \ 1 \leq i \leq k-2 \text{ if } k > 2.
\]

Obviously the actual value of \( f(k) \) for large \( k \) is extremely difficult to obtain. We will attempt to find an easily calculated number above \( f(k) \), but of similar order, which can serve as the upper bound for \( g \).
Since $m_{k-1} = m_k \cdots m_{k-1+1} + 1$ for $1 \leq i \leq k-2$, then

\[ m_{k-1+1} = m_k \cdots m_{k-1+2} + 1 \]

for $2 \leq i \leq k-1$ or $m_{k-1+1} - 1 = m_k \cdots m_{k-1+2}$ and therefore $m_{k-1} = (m_{k-1+1} - 1) (m_{k-1+1}) + 1$ for $2 \leq i \leq k-2$. That is, $m_{k-1} = \frac{(m_{k-1+1}^3 + 1)}{m_{k-1+1} + 1}$

\(< (m_{k-1+1})^2 \)

for $2 \leq i \leq k-2$. Now we had $m_k = 2$, and

\[ m_{k-1} = 2 + 1 = 3, \quad m_{k-2} = 2 \cdot 3 + 1 = 7, \]

and so on. To begin the chain of $m_{k-1} < (m_{k-1+1})^2$, $2 \leq i \leq k-2$, we have $i = 2$, and $m_{k-1+1} = m_{k-1} = 3$, so $m_{k-2} < 3^2$, $m_{k-3} < 3^4$, $\ldots$, $m_2 < 3^{2k-3}$. It follows that for $k \geq 4$ (because of $2 \leq i \leq k-2$), $f(k) = m_k m_{k-1} \cdots m_2 < 2 \cdot 3^2 \cdots 3^{2k-3}$

\[ = 2 \cdot 3^{2k-2} - 1 < 3^{2k-2} \]

For $k = 3$, $f(k) = m_3 m_2 = 3 \cdot 2 = 6$

which is less than $3^{2k-2} = 3^2 = 9$ here; for $k = 2$

then $m_2 \geq 2$ means, solving in (1.1.4), $m_1 = g \leq 2$ which is less than $3^{2k-2} = 3$; for $k = 1$, $G = K_1 = 1$ of order $1$ which is less than $\sqrt{3}$. Hence for all values of $k$,

$g < 3^{2k-2}$

Q.E.D.

Note that in the course of the above proof we had a chain $m_{k-1} < (m_{k-1+1})^2$ ($2 \leq i \leq k-2$) which could have begun instead at $i = 3, 4, \ldots$ and the corresponding

$m_{k-2} = 7, m_{k-3} = 43, \ldots$, in which case in the same way we would have $7^{2k-3} < 43^{2k-4}$, \ldots respectively for the
upper bound of the order $g$ of a group with $k$ classes. Each of these is an improvement on the value in (1.1.8) of $3^{2k-2}$; however, in Chapter 2, we will show that when $k$ is 1, 2, 3, 4, 5, 6, and 7, the maximum order $g$ of a group with $k$ classes is respectively 1, 2, 6, 12, 60, 168, 360, while the corresponding values of $3^{2k-2}$ are 2, 3, 9, 81, 6561, 43046721, and 1853020188851841. Obviously then none of the upper bounds mentioned above is of the order of a least upper bound. In fact it would seem that the least upper bound of the order $g$ of a group with $k$ classes is of the order of $3^{k-1}$.

Although Landau's proof of the existence of an upper bound does not lead apparently to an approximation of the least upper bound, we must keep in mind that no group theory apart from that stated before (1.1.6) is used in obtaining (1.1.8).

Thus the problem this thesis attempts to solve, of finding a least upper bound, under certain restrictions, is one posed by R. Brauer in 1964 ([4], p.137, Problem 3): "Give upper bounds for the order $n$ of a group with a given class number $k$, which lie substantially below the bounds obtainable by Landau's method." Brauer derived the bound 

$$ (2k)^{2k-3} (k-1)^{2k-3} (k-2)^{2k-4} (k-3)^{2k-5} \cdots 4^2 3^2 2^2 (k \geq 3) $$

by
Landau's method; since $(2k)^{2k-3}(k-1)^{2k-3} = (2k(k-1))^{2k-3}$
\[ \geq (2 \cdot 3 \cdot 2)^{2k-3} = 12^{2k-3} > 9^{2k-3} = 3^{2k-2} \quad (k \geq 3), \]
the bound given in (1.1.8) is better.

Other writers (Schmidt [29], Scott [31], Miller [24]) have reproduced Landau's theorem with variations on his method of proof; Miller [24] also states the method of finding the bound $f(k)$, given at the end of (1.1.6). Only Brauer [4] evaluated it.

The importance of the least upper bound of $g$, given $k$, is reflected in the theory of group representations. It has long been known that the number of irreducible representations of a group equals its class number (see Hall [14], p.267). Thus for example given a group $G$ of order $g$, its class number must be greater than some minimum number $r$ by (1.1.6) and (1.1.8) and hence in searching for the irreducible representations of $G$ one must have at least $r$. For other such applications see [4].

The major limitations we place upon the problem of a least upper bound are explored in Chapters 2 and 3.

W.Burnside [8] and G.A.Miller ([23],[24],[26]) restricted $k$ to the values 1, 2, 3, 4, and 5, and derived the corresponding group class equations possible. In Chapter 2
we extend this to cover $k = 6$ and $k = 7$. The basic results are tabulated in section 2.3. (Only one author, Sigley [32], has ever done similar work, for $k = 6$, and his results were incomplete.) In section 2.4 we present the proof of these results, based upon a series of rules developed in section 2.2. The outline of this chapter is similar to that of Burnside's Note A" ([8]). We complete Chapter 2 with a summary of the implications of this work.

The least upper bound of the order $g$ of a group of prime power order with $k$ conjugate classes is found in Chapter 3. The methods employed are distinct both from those of Chapter 1 and of Chapter 2; the result is stated in section 3.2. (My director, Dr.H.Schwertfeger, has kindly shown me recent correspondence with C.Ayoub [40] and J.Rose [41]; Mrs.Ayoub has calculated the least upper bound for $p$-groups up to order $p^6$, and derived a formula (not stated) for the class number of a $p$-group containing an element with maximum number of conjugates (cf.(3.2.3)). Dr.Rose announced that P.Hall has proved (unpublished) that the class number of a group of order $p^{2n+e}$, $n \in \mathbb{Z}_0^+$, $e = 0$ or 1, has the form $p^a + (p^2-1)(n+a(p-1))$ where $a \in \mathbb{Z}_0^+$ (cf.(3.2.1)). Except for an elementary piece in Miller [25], no mention of similar work appears in the
In section 3.3, we examine the formula for minimum class number, for 2-groups, and show that as the order increases, the formula must be revised.

Chapter 4 contains a brief outline of the results of others on the group class equation, not undertaken in the above areas, but perhaps applicable. Except where noted in Chapters 2 and 3, all the work therein is original. Theorem (1.1.8) and the details of the proof of (1.1.6) are also my own work.
Section 1.2: Notation.

For reference, articles in the bibliography are denoted, for example [5], with brackets. Theorems and equations in this paper are denoted with parentheses in a style similar to M.Hall, Jr. [14]. For example, (3.5.7) means the seventh item numbered in the fifth section of the third chapter.

The majority of the notation is standard (see Hall [14], p.433). Upper case letters will denote sets; lower case letters will denote elements or numbers - in particular, p will represent always a prime number.

The following is a brief list of symbols used which either could be ambiguous, are required because there was a conflict in notation, or are not always used standardly.

\[ \{ x \in A \mid * \} \] - the set of all elements \( x \) in \( A \) which satisfy property \( * \),

\[ \langle x, y, \ldots \mid * \rangle \] - the group generated by \( x, y, \ldots \) operating under the relations \( * \),

\( A \leq B \) - \( A \) is a subset (or subgroup if \( A \) and \( B \) are groups) of \( B \),

\( A + B \) - the union of \( A \) and \( B \),

\( A - B \) - the set of those elements of \( A \) not in \( B \),

\( Z(G) = Z \) - the center of \( G \),
The set of all integers, 
the set of all integers \( j > 0 \), 
the set of all integers \( j \geq 0 \), 
the symmetric group of degree \( n \) (see Scott [31], p.474), 
the alternating group of degree \( n \), 
an arbitrary \( p \)-Sylow subgroup of the group \( G \) for a given prime \( p \), 
the number of elements in (the order of) \( A \); 
for elements \( a \) and \( b \) of a group \( G \), 
the order of \( a \), 
\( bab^{-1} \), 
\( a^{-1}b^{-1}ab \) (see Curtis and Reiner [9], p.15); 
for integers \( a \) and \( b \), 
the G.C.D. of \( a \) and \( b \), 
\( p^a \mid b \) but \( p^{a+1} \nmid b \), where \( p \) is a prime (see Curtis and Reiner [9], p.xiii).

For the special problem of this thesis, we always let 
\( k(G) = k \) denote the conjugate class number of a group \( G \), 
\( K_i \) represent the \( i \)th class, and \( K_G(x) = K(x) \) be the class of \( G \) containing \( x \) (see Brauer [4], p.138). This notation follows from the German for class - Klasse. (Such reference to the German is not uncommon; for example, the use of \( Z \) for the center - Zentrum. It is often done for words beginning with \( c \), which abound in algebra.)
Almost all authors use \( h_{1} \) for \(|K_{1}|\), and \( C_{G}(x) = C(x) = N_{G}(x) = N(x) \) for the centralizer (or normalizer) of \( x \) over \( G \). The notion of the centralizer of an arbitrary element of a given class \( K_{1} \) is not often found in the literature, and I have taken the notation \( C_{G}(x \in K_{1}) \) and abbreviated it to \( C(K_{1}) \). Such an idea is similar to that above of \( S_{p} \), an arbitrary Sylow subgroup for a given prime \( p \). As with \( S_{p} \), all \( C(K_{i}) \) for a fixed \( i \) have the same order (if more than one exists) by (1.1.3), and any one is conjugate with any other:

(1.2.1) **Theorem:** If \( x, y \in K_{1} \), then there exists some \( z \in G \) so \( zC(x)z^{-1} = C(zxz^{-1}) = C(y) \).

**Proof:** Since \( x, y \in K_{1} \), let \( z \in G \) be such that \( zxz^{-1} = y \). Then \( C(y) = C(zxz^{-1}) = \{w \in G \mid w(zxz^{-1})w^{-1} = zxz^{-1}\} \)

\[= \{w \in G \mid (z^{-1}wz)x(z^{-1}w^{-1}z) = x\} = \{zuz^{-1} \in G \mid uxu^{-1} = x\} \]

\[= zC(x)z^{-1}, \text{ putting } u = z^{-1}wz \text{ so } w = zuz^{-1}. \]

Q.E.D.

The index of \( K_{1} \) in \( G \), or \(|G|/|K_{1}|\), is more frequently met but the notation varies so greatly, I have taken that or Burnside ([8]) and put \( g/h_{1} = |G|/|K_{1}| = m_{1}. \) I have avoided the notation \( C_{i} \) for \( C(K_{1}) \) and \( c_{i} \) for its order (see Brauer [4], p.140,161) because many authors use this notation for the classes and some structural constants in representation theory (see for example Curtis and Reiner [9], p.234; Hall [14], p.277; or Scott [31], p.329).
Because \((z x z^{-1})^a = z(x^a)z^{-1}\) for \(a \in J\), it follows that conjugate elements have the same order. Let this common order of the elements of \(K_i\) be denoted by \(\text{exp } K_i\), the exponent of \(K_i\). This is similar to the familiar notation of \(\text{exp } G = \min \{a \in J^+ \mid x^a = 1 \text{ for all } x \in G\}\).

Finally, \(F(a,b)\) will denote a Frobenius group. (This notation was introduced in [28]; for the following discussion, references are implicitly to [28].) By a Frobenius group is meant a group \(G\) of order \(g\), containing a proper subgroup \(A\) of order \(a \neq 1\), satisfying \(A \cap xAx^{-1} = 1\) if \(x \notin A\).

A theorem of Frobenius (Burnside [7], p.334) then states that \(G\) contains a characteristic subgroup \(B\) of order \(b = g/a\) consisting of just those elements of \(G\) whose order divides \(b\).

A Frobenius group can be characterized (Feit [10]) too as a group \(G\) of order \(ab\), \((a,b) = 1\), \(a \neq 1 \neq b\), in which every element has order dividing \(a\) or \(b\) and \(G\) has a normal subgroup of order \(b\). If \(G\) is \(F(a,b)\) then \(G\) can be written \(G = A + y_2Ay_2^{-1} + \cdots + y_bAy_b^{-1} + B\) where the \(y_i\) are the distinct elements of \(B\); any two summands intersect in \(1\) and no two elements \((\neq 1)\) of distinct summands commute.

Hence each element not in \(B\) generates an automorphism of \(B\) which leaves only \(1 \in B\) fixed, a so-called fixed-point-free automorphism, denoted \(\text{FPFA}\). It follows that \(a!(b-1)\).

\(A\) and \(B\) are called the complementary and regular subgroups.
CHAPTER TWO
ON BURNSIDE'S NOTE A

Section 2.1: Introduction.

At the end of the second edition of his book "Theory of Groups of Finite Order" [7], W.Burnside wrote a series of notes on topics in group theory open to research such as the orders of simple groups (Note N), groups of odd order being possibly solvable (Note M), and the symmetric group (Note C). The first of these, Note A, was entitled "On the Equation \( N = h_1 + h_2 + \cdots + h_r \)" which is equivalent to the group class equation (1.1.2), using \( N \) for \( g \), the order of the group \( G \), and \( r \) for \( k \), the class number. Note A states some conditions upon the relations between possible values of \( h_1 \) and \( g/h_1 = m_1 \) in order that (1.1.2) or (1.1.4) correspond to actual groups; it continues, listing the class equations for groups with class number \( k \leq 5 \), and generalizes for two types of groups which occur frequently in taking successive values for \( k \). The purpose of this chapter is to continue Burnside's work in these areas.

We consider only non-abelian groups, since in an abelian group \( xyx^{-1} = y \) for all \( x \) and \( y \), so each \( h_1 = 1 \), each \( m_1 = g \), and \( k(G) = g \). Conversely, \( k(G) = g \), all \( m_1 = g \), and all \( h_1 = 1 \) are equivalent and they imply that \( G \)
is abelian. Indeed, the equivalence follows from (1.1.2) and (1.1.4), while all \( m_i = g \) implies that each element commutes with all of \( G \), the definition of an abelian group. In fact, the case of abelian groups is at the opposite extreme to the problem considered in this thesis. For an abelian group, \( k(G) = g \) and no group can have \( g = |G| < k(G) \), as is seen in the group class equation (1.1.1), since no \( K_i \) is empty. Therefore abelian groups are exactly those groups which, for a given class number \( k \), have the minimum possible order; our interest will be in groups which have the maximum possible order. For this reason, and also because they are easily classified (given \( k \), then \( |G| = k \), and the defining relations of \( G \) follow as in Burnside [7], Chapter VII), we will examine just the case of \( k < |G| \), \( G \) non-abelian.

In the next section, 2.2, we develop a series of theorems whose immediate object is to aid in the proof of the results stated in 2.3, a list of those groups with \( k \leq 7 \). Some of the theorems in 2.2 will be referred to in Chapter 3; we hope they also will form a basis for further work, on \( k \geq 8 \). The proof that the groups stated in 2.3 are the only ones for \( k \leq 7 \) is presented in 2.4. Lastly, in 2.5 we mention some inferences drawn from the list in 2.3.
Section 2.2: Conditions Upon The Group Class Equation.

We begin with a useful and easily proved theorem connecting centralizers.

(2.2.1) Theorem: \( C_G(x) \leq C_G(x^a) \) with equality if \((a, |x|) = 1\).

Proof: If \( z \in C_G(x) \) then \( zxz^{-1} = x \). Therefore \( z(x^a)z^{-1} = (z(xa))z^{-1} = xa \) so \( z \in C_G(x^a) \). If in addition \((a, |x|) = 1\), then there exist integers \( s \) and \( t \) so that \( sa + t\cdot |x| = 1 \) and hence \((x^a)^s = x^{1-t\cdot |x|} = x \). Therefore \( C_G(x^a) \leq C_G(x) \) and we are done.

Q.E.D.

For our first examination of the group class equation (1.1.4) \( \frac{1}{m_1} + \cdots + \frac{1}{m_k} = 1 \), we have the following broad result.

(2.2.2) Theorem: Let \( m_j = p_1^{a_1} \cdots p_n^{a_n} \) be the prime decomposition of \( m_j \), and let \( n > 1 \). Then for a given \( j \) (\( 1 \leq j \leq n \)) either any element of \( C(K_j) \) of order \( p_1^{b_1} \) (any \( b_1 \in \mathbb{Z}^+ \)) commutes with an element of relatively prime order, or \( |Z(C(K_j))| \) divides \( p_1^{a_1} \) and \( a_1 > 1 \).

Proof: Let \( x \in K_j \) so that \( C(K_j) = C_G(x) \); let \( |y| = p_1^{b_1} \), \( y \in C(x) \). Then \( y \) commutes with \( x \) and hence \( x^{p_1^{a_1}} \) by (2.2.1), and, unless \( x^{p_1^{a_1}} = 1 \), \( x^{p_1^{a_1}} \) must have order relatively prime to \( p_1 \). If \( x^{p_1^{a_1}} = 1 \), suppose \( a_1 = 1 \), so \( x^{p_1} = 1 \); then \( |y| = p_1 \) too, and \( Z(p_1(C(x))) = \langle x \rangle \leq Z(C(x)) \). This
means \( S_{p_1}(C(x)) \triangleleft C(x) \) and hence unique. But then
\( y \in S_{p_1}(C(x)) \), so \( y = x^a \), \((a, p) = 1\). By (2.2.1), \( C(y) = C(x) \). It follows that \( y \) must commute with an element of order prime to \( p_1 \) because \( n > 1 \).

Q.E.D.

(2.2.3) Note: In all discussions of \( m_i \), \( b_i \), or \( K_i \) in this section, we take \( i > 1 \), unless we explicitly include the case \( i = 1 \).

The early writers (Burnside [8] and Miller [23]) were quick to note a most important relation on the \( m_i \).

(2.2.4) Theorem: If \( m_1 = p \), \( p \) prime, then \( g = pr \), \((r, p) = 1\), and if \( plm_j \) then \( m_j = p \).

Proof: If \( x \in K_1 \), then \( |C(x)| = p \) so \( C(x) = \langle x \rangle \). But since \( |x| = p \), \( x \) must be contained in some \( p \)-Sylow subgroup \( S_p \) of \( G \). Naturally \( 1 \not\in Z(S_p) \triangleleft C(x) = \langle x \rangle \). Hence \( Z(S_p) = \langle x \rangle \), which implies that \( S_p \triangleleft C(x) = \langle x \rangle \) so \( |S_p| = p \).

By (2.2.1) then \( S_p \) is the centralizer of every non-trivial element in it. This is characteristic therefore of all \( p \)-Sylow subgroups of \( G \) and it follows that no element of order \( p \) commutes with an element of another order. By (2.2.2), if \( plm_j \) then \( m_j = p \).
(2.2.5) **Theorem:** $G$ is a Frobenius group of type $F(p,g/p)$ if and only if $m_i = p$ for $p-1$ distinct values of $i$.

**Proof:** If $G = F(p,g/p)$ let $x \in G$ so $|x| = p$. Then $x$ can only commute with the elements in the same complementary subgroup as itself, and since this is $\langle x \rangle = S_p$, then $G(x) = \langle x \rangle = S_p$. Hence some $m_i = p$. Now distinct elements of $S_p$ are conjugate over $G$ if and only if they are conjugate over $S_p$ (because $G$ is a Frobenius group), which is impossible since $S_p$ is cyclic. Thus there must be at least $p-1$ distinct conjugate sets with $m_i = p$. There cannot be more by (1.1.4) unless $|G| = p$, a contradiction.

Conversely, $m_i = p$ means $p | g$ by (2.2.4) so the intersection of pairs of distinct $p$-Sylow subgroups must be trivial. As the number of elements of order $p$ is $(p-1)|K_i| = (p-1)\cdot(g/p)$, there must be $g/p$ $p$-Sylow subgroups, and therefore $|N_G(S_p)| = p$ (see Burnside [7], p.151). By the Theorem of Frobenius, $G$ is $F(p,g/p)$.

**Q.E.D.**

Miller [23] states the above theorem in a lesser form, and although no mention is made in Burnside [8], he surely knew of it too. The number of classes of a Frobenius group can be determined by the following formula.
(2.2.6) **Theorem:** If $G$ is a Frobenius group of type $F(a,b)$ with complementary subgroup $A$ and regular subgroup $B$, then
\[ k(G) = k(A) + \frac{k(B)-1}{a}. \]

**Proof:** Recall that $G = A + y_2 Ay_2^{-1} + \cdots + y_b Ay_b^{-1} + B$, summands having trivial intersection, where $B = \{1, y_2, \ldots, y_b\}$. No element of any $y_1 Ay_1^{-1}$ can be conjugate with an element of $B$ since the former have orders dividing $a$ and the latter dividing $b$, while $(a, b) = 1$. Further, since $A$, $y_2 Ay_2^{-1}$, $\ldots$, $y_b Ay_b^{-1}$ are all possible complementary subgroups of $G$ and two elements of $A$ are conjugate over $G$ if and only if they are conjugate over $A$, the number of conjugate classes of $G$ in $A + y_2 Ay_2^{-1} + \cdots + y_b Ay_b^{-1}$ is $k(A)$. There remain the classes of $G$ composing $B - 1$. Since no element of $B - 1$ commutes with any element not in $B$, $x \in B - 1$ implies that $C_G(x) = C_B(x)$ and hence $|K_G(x)| = g/|C_B(x)| = \frac{ab}{|C_B(x)|} = a \cdot |K_B(x)|$. Therefore $B - 1$ splits into $[k(B)-1]/a$ classes over $G$.

Q.E.D.

With this result, we may easily prove a theorem of Burnside [8] that if $m_k = 2$ then the group class equation (1.1.4) has a unique solution, $m_j = 2k-3$ ($j \neq k$), or more precisely:
(2.2.7) **Theorem:** If \( m_1 = 2 \), then \( i = k \), \( m_j = 2k-3 \) \( (1 \neq j \neq k) \), \( G = F(2,2k-3) \), and such a group exists for all \( k > 2 \).

**Proof:** Since \( m_1 > m_2 > \cdots > m_k > 2 \), then \( m_k = 2 \), and \( m_{k-1} \neq 2 \) for otherwise \( k = 2 \), \( g = 2 \), and \( G \) would be abelian. By (2.2.5), \( G = F(2,g/2) \). Since the order of the complementary subgroup is 2, even, the regular subgroup \( B \) is abelian of order \( b \) (Burnside [7], p.172) and using (2.2.6), \( k = k(G) = (2 - 1) + \frac{(m - 1)}{2} \) so \( m = 2k - 3 \) and \( G \) is \( F(2,2k-3) \). From the discussion in (2.2.6), the elements not in the \( C(K_k) \) are exactly those of \( B \), and so \( x \in B - 1 \) implies \( |C(x)| = |B| = 2k-3 = m_j \) for \( 1 \neq j \neq k \). The group \( G = \langle a,b \mid a^2 = 1, b^{2k-3} = 1, b^a = b^{-1} \rangle \) exists, is \( F(2,2k-3) \) if \( k > 2 \), and has the required class equation.

Q.E.D.

This shows that non-abelian groups exist having a conjugate class number equal to any given integer greater than two. This condition is an obvious one, as we can show.

(2.2.8) **Theorem:** \( 2 \leq m_k \leq k - 1 \).

**Proof:** Suppose \( m_k > k \). Then by (1.1.5) \( g = m_1 \geq m_2 \geq \cdots \geq m_k \geq k \)

so in (1.1.4) \( \frac{1}{m_1} + \cdots + \frac{1}{m_k} \leq \frac{1}{k} + \cdots + \frac{1}{k} \leq 1 \) with equality if and only if \( g = m_1 = \cdots = m_k = k \); that is \( G \) is abelian of order \( k \), a contradiction. By (1.1.5), \( m_k \geq 2 \).

Q.E.D.
(2.2.9) **Corollary:** No non-abelian groups exist with \( k \leq 2 \).

The following discussion is too unwieldy to be placed in the format of a theorem.

(2.2.10) **Note:** If \( x \) is an element of \( G \) of order \( n = 2^{a_0} p_1^{a_1} \cdots p_r^{a_r} \), where the \( p_i \) are distinct odd primes, then the group \( A_x \) of automorphisms of \( \langle x \rangle \) is the direct product of cyclic groups of order \( p_i^{a_i-1}(p_i - 1) \), as well as cyclic groups of order 2 and \( 2^{a_0-2} \) provided \( a_0 \geq 2 \) (see Scott [31], 5.7.12, or Burnside [7], section 88). Denote by \( u_x \in A_x \) the product of the generators of the cyclic direct factors of \( A_x \). The order of \( u_x \) is the \( \text{LCM} \) of the orders of the generators which is also \( \exp(A_x) \).

\( |A_x| \) represents the number of powers of \( x \) which have order \( n \). Let \( k_G(x^a;n) \) denote the number of classes of \( G \) containing a power \( x^a \) of \( x \) with order \( n \).

(2.2.11) **Theorem:** \( |u_x| \) can be written as a product \( b \cdot c \) so

(i) \( c \) is the order of some element of \( G \), (ii) \( c \mid G \),

(iii) \( b \mid k_G(x^a;n) \), and (iv) \( k_G(x^a;n) \mid \exp(A_x)/c \).

**Proof:** Let the image \( u_x(x) \) of \( x \) under the automorphism \( u_x \) be \( x^y \). Let \( b \) be the smallest positive integer such that

\[ u_x^b(x) = x^{b} \in K_G(x) = K(x). \]

Then \( x^b = y x^y y^{-1} \) for some \( y \),
and \( y^d x^{-d} = x^{vb} \in K(x) \). Suppose \( x^v \in K(x) \) but \( v \not\equiv 0 \) modulo \( b \), and let \( zxz^{-1} = x^v \). Take integers \( s \) and \( t \) so \( s \cdot b + t \cdot e = (b,e) < b \) (since \( b/e \)); then \( y^t z^s(x)z^{-s}y^{-t} = x^{vsb+te} = x^v(b,e) \in K(x) \), contradicting the choice of \( b \).

Let \( c = \lfloor u_x \rfloor / b \); note that \( x^{vb} = u_x^{u_x}(x) = x \) and \( c \) is the smallest such positive integer. Again if \( x^{vb} = x \) then \( \lfloor u_x \rfloor = bc \) be or c\( e \). Now \( x = y^1y^1x_y^1y^1 = x^{vb}y^1 \) so \( c \mid o(y) \). It follows that \( y^1y^1/c \in g \) has order \( c \), and \( c \mid g \) of course.

Next \( x^f, x^{fv}, x^{fv^2}, \ldots, x^{fv^{b-1}} \) are in distinct classes for any \( f \) satisfying \( (f,n) = 1 \); indeed if \( w(x^{fv^i})w^{-1} = x^{fv^j} \) for some \( 0 \leq i < j < b \), then \( (wxw^{-1})^{fv^i} = x^{fv^j} \) or, taking \( s \) and \( t \) so \( sf + tn = (f,n) = 1 \) as usual, \( (wxw^{-1}) = (wxw^{-1})(1-tn)(v^i-1) = (wxw^{-1})^{fv^i(sv^{-1})} = (x^{fv^j})^{sv^{-1}} = x^{(1-tn)v^j-1} = x^{v^j-1} \), contradicting the choice of \( b \), since \( 0 < j-1 < b \). Hence the \( (bc) \) images of \( x \) under the powers of \( u_x \) fall into \( b \) distinct conjugate sets of \( c \) elements each.

If \( x^f \) is any power of \( x \) with order \( n \) which is not the image of \( x \) under some power of \( u_x \), then this process may be repeated, of course. The essence of the repetition is that
(f,n) = 1 so there exist integers s and t such that sf+tn=1; then any equation involving \((x^f)\) is raised to \((x^f)^s = x^{1-tn} = x\) and reverts to the case above. For example, the images of \(x^f\) under \(u_x\) powers, conjugate to \(x^f\), are \(y^i x^f y^{-1}\), \(0 \leq i < \phi\), and \(b\) is the smallest integer > 0 such that \((x^f)^b \in K(x^f)\).

In order to prove that \(b k_G(x^a : n)\) and \(c k_G(x^a : n)\) divides \(|A_x|\) let \(x^a\) be conjugate to \(x^j = u_x^j(x)\) for some \(j\), \((e,n) = 1\), but \(x^a\) not an image of \(x\) under a power of \(u_x\). Then \(z x^a z^{-1} = x^j\), and \(z(x^a)^{y^b} z^{-1} = (z x^a z^{-1})^{y^b} = x^{j+bi}\). Hence for this \(e\), we have increased to \(c+c = 2c\) powers of \(x\) of order \(n\) in \(b\) conjugate sets. On the other hand, if we take \(x^f\) not conjugate to any \(x^j\), \((f,n) = 1\), then no image of \(x^f\) under \(u_x\) powers will be conjugate to any \(x^j\) (since \(z x^f z^{-1} = x^j\) if and only if \(z x^f z^{-1} = x^{j-1}\) and we have increased the number of classes containing powers of \(x\) of order \(n\) to \(b+b = 2b\), while maintaining \(2c\) powers of \(x\) of order \(n\) in each (since \(w x^a w^{-1} = x^j\) implies \(w x^f w^{-1} = x^f x^j\)).

Continuing this until all such powers of \(x\) are exhausted, we have at last \(k_G(x^a : n)\) = the number of classes of \(G\) containing \(x^a\) for some \(a\) prime to \(n\) is a multiple of \(b\), and all the powers of \(x\) of order \(n\), namely \(|A_x|\), fall into these \(k_G(x^a : n)\) classes containing a multiple of \(c\) such powers each.

Q.E.D.
(2.2.12) **Corollary:** \( k_\sigma(x^a:m) \) is a multiple of \( l_{u(x)}/(g,l_{u(x)}) \).

**Proof:** Actually \( \frac{l_{u(x)}}{(g,l_{u(x)})} = \frac{bc}{(g,bc)} = \frac{cb}{c(g,b)} \), divides \( b \).

Q.E.D.

Now Miller ([25]) has shown:

(2.2.13) **Theorem:** The number of distinct values of \( i \) for which \( m_1 = p \) (a prime) is a divisor of \((p-1)\) and its quotient \( (p-1)/b \) of \((p-1)\) is the order of some element.

**Proof:** If \( x \in K_1 \) where \( m_1 = p \), then \( <x> = C(x) = S_p(G) \) by (2.2.4). Here, \( |A_x| = l_{u(x)} = p-1 \). Since by (2.2.11) \( l_{u(x)} = bc \cdot k_G(x^a:p) \cdot o(A_x) \), then \( k_G(x^a:p) = b \), a divisor of \( p-1 \), and \( (p-1)/b = c \) is the order of an element of \( G \).

Finally, since \( <x> = S_p(G) \), every element of order \( p \) which is not a power of \( x \) is conjugate to a power of \( x \), so the number of conjugate sets for elements of order \( p \), or the number of \( m_1 = p \), equals \( k_G(x^a:p) \).

Q.E.D.

(2.2.14) **Corollary:** If \( m_1 = p \) for only one value of \( i \), then \( G \) contains an element \( x \) of order \((p-1)\).

(2.2.15) **Theorem:** Suppose \( m_1 \) and \( m_j \) are odd primes such that \( m_j \mid (m_1-1) \) and \( m_1 + 1 \neq m_j \). Then \( m_1 - 1 = m_i \).
Proof: Obviously $i < j$ by (1.1.5). Suppose $m_{i-1} \neq m_i$ so that, again by (1.1.5), $m_t \neq m_i$ if $t \neq i$. By (2.2.14) then $G$ contains an element $x$ of order $m_i - 1$, so $(m_i - 1) \mid o(C_G(x))$ which must be some $m_t$. But then the prime $m_j \mid m_t$. By (2.2.4) $m_t = m_j$ so $m_i - 1 = m_j$, contradicting $m_i$ and $m_j$ odd. Therefore $m_{i-1} = m_i$.

Q.E.D.

On the other hand, if the index of some class of $G$ is composite we have the following conditions.

(2.2.16) Theorem: If $m_i = pq$, $p$ and $q$ unequal primes, then for at least three distinct values of $j$, $pq \mid m_j$.

Proof: If $m_i = pq = |C_G(K_i)|$, then $x \in K_i$ has order $pq$, $p$, or $q$. If $|x| = pq$, then $x$ is contained in $C_G(x^q)$ and $C_G(x^p)$, which therefore have orders divisible by $pq$, and since $|x^q| = p$ and $|x^p| = q$, $K(x^q)$, $K(x^p)$, and $K(x)$ are distinct. Suppose now that $|x| = p$. Then $x$ commutes with an element $y$ of order $q$, so $x \in C_G(y)$ while $K(y) \neq K(x)$. Further, $|xy| = pq$ since $x$ and $y$ commute; therefore $K(x)$, $K(y)$, and $K(xy)$ are distinct, and $pq$ divides their indices in $G$. The case of $|x| = q$ is identical with that of $p$, so we have finished the proof.

Q.E.D.
(2.2.17) **Theorem:** If the prime decomposition of \( m_t \) is \( p_1^{a_1} \cdots p_n^{a_n} \) with \( n > 1 \), then for each \( p_i \) there exists a prime \( p_f(i) \neq p_i \), and values \( j(i), j'(i) \), mutually distinct and distinct from \( t \), such that \( p_1 p_f(i) \) divides \( m_j(i) \) and \( m_{j'}(i) \).

**Proof:** Take any \( p_i \) and an element \( x \) of \( C_G(K_t) \) of order \( p_i \). If \( o(Z(C_G(K_t))) \nmid p_1^{a_1} \) then by (2.2.2) an element \( y \) of \( C_G(K_t) \) of order \( p_f(i) \neq p_i \) exists which commutes with \( x \), from which the theorem follows, as in (2.2.16), by taking, with \( K_t = K(x), \ K_j(1) = K(xy) \) and \( K_{j'}(1) = K(y) \) which are mutually distinct because \( |x|, |xy|, \text{and} \ |y| \) are, and of course \( p_1 p_f(i) \) divides their indices in \( G \).

If \( o(Z(C_G(K_t))) \mid p_1^{a_1} \), take \( x \in Z(C_G(K_t)) \). Since \( n > 1 \), elements of prime order (not \( p_1 \)) exist in \( C_G(K_t) \) and they commute with \( x \). Again, for such an element \( y \), we take \( K_j(1) = K(xy) \) and \( K_{j'}(1) = K(y) \) and the proof is complete.

Q.E.D.

(2.2.18) **Theorem:** If the prime decomposition of \( m_t \) is \( p_1^{a_1} \cdots p_n^{a_n} \), then \( k \geq 2n \).

**Proof:** Renumbering if necessary, we can take \( x \in Z(C_G(K_t)) \) with order \( p_1 \). If \( y \in C_G(K_t) \) with \( |y| = p_2 \), then \( x \) and \( y \) commute so \( K(x), K(y) \) and \( K(xy) \) are distinct by \( x, y, \text{and} \ xy \).
having distinct orders $p_1$, $p_2$, and $p_1p_2$ respectively. If we next take $z \in C_G(K_t)$ so $|z| = p_3$, then $K(z)$ and $K(xz)$ are distinct from the above three, since $z$ and $xz = zx$ have orders $p_3$ and $p_1p_3$. Continuing, we get $1 + 2(n - 1) = 2n - 1$ classes. Since none is $K_1$, $k > 2n$. Even if $n = 1$, we have seen in (2.2.9) that $k > 2$.

Q.E.D.

(2.2.19) Theorem: If $k$ is an even number, then so is $g$.

Proof: Suppose $k$ is even and $g$ is odd. Then in the group class equation (1.1.2) $h_1 + h_2 + \cdots + h_k = g$, all $h_i$, dividing $g$ by (1.1.3), must be odd. However $h_1 + \cdots + h_k$, as a sum of an even number of odd numbers, must be even which is a contradiction.

Q.E.D.

The next theorem (Burnside [7], p.36) we state without proof.

(2.2.20) Theorem: If $H \subseteq G$, then there exists a set $S$ of integers between 1 and $k$, with $1 \in S$, such that $|H| = \sum_{s \in S} h_s$ and if $x \in K_s$, $s \in S$, then $x \in H$.

We consider now the relationship between the conjugate classes of $G$ and $G/H$. 
Note: Let \( l \neq H < G \). Let \( A_1 = a_{11}H + a_{21}H + \cdots + a_{f(1)}H \) where \( f(1) = 1 \) and \( a_{11} = 1 \), and if all \( A_j \) are defined for \( j < 1 \), let \( a_{11} \) be any element of \( G - (A_1 + \cdots + A_{1-1}) \), denote \( a_{11} \) by \( a_1 \), let \( a_{21} \) be any element of \( K(a_1) - a_{11}H \), let \( a_{31} \) be any element of \( K(a_1) - a_{11}H - a_{21}H \), and so on until \( f(1) \) is the minimum integer such that \( K(a_1) \leq A_1 \); note that \( K(a_1) > \{ a_{j1} : 1 \leq j \leq f(1) \} \). Continuing in this manner, we exhaust \( G \). Let \( k \) be the number of \( A_1 \). Without loss of generality we assume the \( A_1 \) are numbered such that \( H = A_1 \) and \( |A_1| \leq |A_{j1}| \) if \( i < j \). The choice of values for the \( a_{j1} \) is now fixed.

Theorem: \( |A_1| = f(1) \cdot |H| \).

Proof: We need to show \( a_{j1}H \cap a_{j1}'H \) is empty if \( j \neq j' \), say \( j' < j \). But \( a_{j1}x = a_{j1}'x' \) for \( x, x' \in H \) means \( a_{j1} \in a_{j1}'H \); this contradicts the choice of \( a_{j1} \) in (2.2.21).

Q.E.D.

Theorem: Each \( A_1 \) is the set of all conjugates of the elements of \( a_{11}H \).

Proof: Take \( a_{j1}x \in A_1, x \in H \). Then \( a_{j1}x = w(a_1)w^{-1} \cdot x = w(a_1x^*)w^{-1} \) for some \( w \in G \), by the construction in (2.2.21), and where \( w^{-1}x = x^w \) or \( x^* = w^{-1}xw \in w^{-1}Hw = H \). Therefore
every element of $A_i$ is conjugate to an element of $a_i H$. But conversely, the conjugates of $a_i x$, $x \in H$, are of the form $w(a_i x)w^{-1} = (w a_i w^{-1})(w x w^{-1}) \in (A_i) \cdot (H) = A_i$

Q.E.D.

(2.2.24) Corollary: Each $A_i$ is the union of classes of $G$.

(2.2.25) Theorem: $A_1$, $A_2$, ..., $A_k$ are disjoint.
Proof: From (2.2.23) we need only show that no $a_i x$ is conjugate to any $a_i', x'$ ($i \neq i'$, say $i' < i$) for $x$, $x' \in H$.
But if it were, then $a_i$ would be contained in $A_i x^{-1} \subseteq A_i H = A_i'$, contradicting the choice of $a_i$ in (2.2.21).

Q.E.D.

(2.2.26) Corollary: If $a_j x$ and $a_j', x'$ are conjugate, $i = i'$.

Let $G \to \overline{G}$ be the canonical homomorphism of $G$ onto $G/H$, and let $x$ represent the image of $x \in G$ under this map. Let $\overline{A}_i$ be the image of $A_i$; that is, $\overline{A}_i = \{ \overline{x} \mid x \in A_i \}$. Directly, using (2.2.23) and (2.2.26), we have:

(2.2.27) Theorem: $\overline{A}_1 = k_G(\overline{A}_1)$; $\overline{1} = \overline{A}_1$, $\overline{A}_2$, ..., $\overline{A}_k$ are the classes of $\overline{G}$; and $\overline{k} = k(\overline{G})$.

Since $H \vartriangleleft G$, $H$ is a union of classes of $G$ and, by $\text{leqH}\neq 1$, $H$ must split into at least two classes over $G$. But then so does $A_1 = H$. From (2.2.24) we have the following theorem, stated in Miller [25].
(2.2.28) Theorem: If \(1 \neq H \triangleleft G\), then \(k(G) > k(G/H)\).

In the case \(H = Z\), we can show:

(2.2.29) Theorem: \(k(G) - |Z| \geq k(G/Z) - 1\), with equality if and only if \(xZ \triangleleft K(x)\) for every \(x \in G - Z\).

Proof: If \(Z = 1\) we are done. If \(Z \neq 1\), then by (2.2.21), \(k(G) - |Z|\) is the number of classes into which the elements of \(G - Z\) split over \(G\); that is, the elements of \(A_2, A_3, \ldots, A_k\). By (2.2.24) there must be at least \(k - 1\) classes here and the inequality follows from (2.2.27), with equality if and only if each \(A_i, i \neq 1\), is a complete conjugate set of \(G\). This is true if and only if for each \(x \in G - Z, K(x) \geq xZ\) (see (2.2.23)).

Q.E.D.

(2.2.30) Theorem: Let \(G\) be partitioned with respect to \(Z\) as in (2.2.21). If \(y, y' \in A_1\) then \(|K(y)| = |K(y')|\).

Proof: By (2.2.23), \(K(y) = K(a_1x)\) and \(K(y') = K(a_1x')\) for some \(x, x' \in Z\). But then \(C_G(a_1x) = C_G(a_1) = C_G(a_1x')\).

Q.E.D.

We have seen in (2.2.8) that \(2 \leq m_k \leq k - 1\). In [8], Burnside attempts to obtain general results for \(G\) if \(m_k = 2\) and if \(m_k = k - 1\), the extremes. The former was
presented in (2.2.7). In the latter case, Burnside said, using the symbol \( r \) for \( k \) (the number of classes):

If \( m_r = r-1 \), the greatest possible value of \( m_1 \) is clearly \( r(r-1) \), and the corresponding solution of the equation is \( m_1 = r(r-1), m_2 = r, m_3 = m_4 = \cdots = m_r = r-1 \).

Hence if the order of the subgroup which contains an operation of the greatest conjugate set self-conjugately is \( r-1 \), the order of the group cannot exceed \( r(r-1) \). When \( r \) is the power of a prime, there are always groups corresponding to this solution (section 140).

We will show that there are two and only two solutions of the group class equation (1.1.4) when \( m_k = k-1 \): (i) \( k = p^a \) (\( p \) prime, \( a \in \mathbb{Z}^+ \)), \( m_1 = p^{a-1} (i \geq 2) \), \( m_2 = p^a \), and \( G \) is \( F(p^a-1, p^a) \) with cyclic complementary subgroups and elementary abelian regular subgroup (Burnside's solution); (ii) \( k = 2^{2n+1} (n \in \mathbb{Z}^+), m_1 = 2^{2n} (i \geq 2), m_2 = 2^{2n+1}, \) and \( g = 2^{2n+1} \) with \( g' = \mathbb{Z} \) of order 2. For such values of \( k \), we show that such groups always exist; in fact, if \( k \) is a Fermat prime then both solutions exist simultaneously. See section 2.3 for the first case, \( n = 1 \).

Unfortunately the proof requires about ten pages, from theorem (2.2.31) to theorem (2.2.46) inclusive. The first stage is to show that \( m_1 = k-1 \) if \( i \geq 2 \), and rewrite \( m_2 \) as \( t + k - 1 \), with \( t \mid k-1 \). Next we do the cases of \( m_2 = k \), its minimum possible value, and \( m_2 = 2(k-1) \), its maximum,
arriving at the solutions stated above. Finally we must prove that \( m_2 \) cannot have any intermediate value. For this, we examine the prime divisors of the \( m_1 \), reducing the class equation; and then we use an argument which is a mixture of methods of N. Ito and of R. Brauer and K. Fowler, to produce a contradiction.

(2.2.31) Theorem: If \( m_k = k-1 \), then \( m_1 \leq \frac{i(k-1)}{(i-1)} \leq 2(k-1) \) for \( i \geq 2 \).

Proof: \[ \frac{1}{m_1} \geq \frac{1}{m_1} + \cdots + \frac{1}{m_1} = 1 - \left( \frac{1}{m_1} + \frac{1}{m_{k-1}} + \frac{1}{m_{k-2}} + \cdots + \frac{1}{m_{i+1}} \right) \geq 1 - \frac{k-1}{k-1} = \frac{i-1}{k-1} \], using (1.1.5) in (1.1.4). Solve for \( m_1 \), restricting \( i \neq 1 \) obviously, and in accord with (2.2.3) too. Q.E.D.

(2.2.32) Theorem: If \( m_k = k-1 \), then \( m_3 = m_4 = \cdots = m_k = k-1 \).

Proof: For the purpose of this theorem we denote \( k-1 \) by \( a \).

By (2.2.31), for \( i \geq 2 \), \( m_1 = a + b_1 \) where \( b_1 \leq a \). Note that \( (a, m_1) = (a, a + b_1) = (a, b_1) \leq b_1 \). Let \( b \) be the minimum value of \( b_1 \) which is not zero, so that for some \( j \),

\[ m_j = a + b, \quad m_{j+1} = m_{j+2} = \cdots = m_k = a \].

Denote \( (a, b) \) by \( b' \leq b \).

With respect to (1.1.4) we have

\[ \frac{b'}{(a+b)a} + \frac{1}{a+b} + \frac{a-1}{a} \geq \frac{b'}{(a+b)a} + \left( \frac{1}{m_2} + \cdots + \frac{1}{m_j} + \frac{1}{m_{j+1}} + \cdots + \frac{1}{m_k} \right) \geq \frac{1}{m_1} + \cdots + \frac{1}{m_k} = 1 \]

since \( m_1 = g = \text{LCM} \{m_1 \neq m_j\} = \text{LCM} \{a, a+b, \ldots\} \geq \text{LCM} \{a, a+b\} \)
\[ = \frac{a(a+b)}{b}. \] We wish to solve this inequality for \( j \). Then
\[ b' + j \cdot a + (a-j)(a+b) \geq a(a+b) \] or \( b' - j \cdot b \geq 0 \). Therefore
\[ j \leq b'/b \leq 1 \] so we must have \( j = 1 \) since \( j \in J^+ \); this implies that \( a-1 = k-2 \) of the \( m_i \) are equal to \( k-1 \) and by (1.1.5) we are done.

Q.E.D.

(2.2.33) **Note:** Let \( m_2 = t + k - 1 \), \( 1 \leq t \leq k-1 \), possible by (2.2.31) \( t = 0 \) is clearly impossible). But then the group class equation (1.1.4) becomes
\[
\frac{(k-1,t+k-1)}{(t+k-1)(k-1)} + \frac{1}{(t+k-1)} + \frac{k-2}{k-1} = 1
\]
which reduces to
\[
(k-1,t+k-1) = t; \quad \text{that is, } t \mid (k-1). \quad \text{Put } y = (t+k-1)/t \quad \text{so that } (t+k-1) = ty, \quad (k-1) = t(y-1).
\]
The class equation reads
\[
\frac{1}{y(k-1)} + \frac{1}{ty} + \frac{k-2}{k-1} = 1.
\]
Since \( t = (t+k-1,k-1) = (ty,k-1) = t(y,k-1/t) \), then
\[
(y,k-1/t) = 1.
\]

(2.2.34) **Theorem:** If \( m_k = k-1 \) and \( m_2 = k \), then \( k = p^a \)
\((p \text{ prime, } a \in J^+)\), \( G = F(p^a-1,p^a) \), the complementary subgroups of order \( p^a-1 \) are cyclic, and the regular subgroup of order \( p^a \) is elementary abelian. Such a group exists for every such value of \( k \) (>3).
Proof: Referring to (2.2.33) we have \( t = 1 \) and \( k = t(y-1)+1 = y; \) (1.1.4) becomes \( \frac{1}{k(k-1)} + \frac{1}{k} + \frac{2}{k-1} = 1. \) If a prime \( p \) divides \( k \) then \( p \not| (k-1) \) so the elements in \( K_2 \) must have order \( p \), since such elements exist in \( G \), and if they were in \( K_1 \) then \( p \mid m_1 \). Since this is true for every prime dividing \( k \) and since \( \exp K_2 \) is fixed, \( k \) cannot be composite.

Let \( m_2 = k = p^a \), a prime power. Every element of \( G \) has order dividing \( p^a \) or \( p^a-1 \), by the values of the \( m_i \); and the elements of order \( p^a \) form a characteristic subgroup since there are exactly \( p^a \) solutions (the elements of \( K_1 \) and \( K_2 \)) of \( x^{p^a} = 1 \) and \( G \) has a subgroup of order \( p^a \), namely \( C(K_2) \).

By a theorem of Feit [10] (or see section 1.2), \( G = F(p^a-1, p^a) \). By a theorem of Burnside ([7], p.182), the regular subgroup of order \( p^a \) is elementary abelian. If \( A \) is a complementary subgroup of \( G \) of order \( p^a-1 \), and \( x \in A \), then \( A \) is the unique subgroup of \( G \) of order \( p^a-1 \) containing \( x \) since \( G \) is a Frobenius group. But \( m_3 = \cdots = m_k = p^a-1 \), so we must have \( x \in Z(A) \); therefore \( A \) is abelian, and hence cyclic (see Zassenhaus [39]). Burnside ([7], section 140) has shown that for all prime powers \( p^a \geq 3 \) such a group exists.

Q.E.D.
(2.2.35) **Theorem:** If \( m_k = k-1 \) and \( m_2 = 2(k-1) \), then \( k-1 \) is a power of 2, \( G \) is a 2-group of order \( 2(k-1) \), \(|G'| = |Z| = 2\), \( \log_2(g) \) is an odd integer, and such a group exists for \( k = 2^{2n} + 1 \) for each \( n \in J^+ \).

**Proof:** The class equation (1.1.4) is \( \frac{2}{2(k-1)} + \frac{k-2}{k-1} = 1 \), by (2.2.32). Therefore \( |Z| = 2 \) and for \( i > 2 \), \( |K_i| = 2 \) so each \( C(K_i) \) is normal and maximal in \( G \). \( Z \) must be the intersection of all \( C(K_i) \); indeed, \( Z \leq \text{all } C(K_i) \) as usual, and if \( z \in \cap C(K_i) \), and \( y \in G \), then \( C(y) \) is some \( C(K_i) \) and thus \( y \) commutes with \( z \). If \( C(x \in K_i) \neq C(y \in K_j) \), then \( G = \langle C(x) , C(y) \rangle \); hence by the isomorphism theorem (Scott [31], p.32), \( G/C(y) \sim C(x)/C(x) \cap C(y) \) or \( C(x) \cap C(y) \) has index 2 in \( C(x) \). Continuing, adding one centralizer at a time, then \( \cap C(K_i) = Z \) has index \( 2^a \) in \( C(x) \) for some \( a \in J^+ \), which means that \( G \) has order \( 2^{a+2} \), and \( k-1 = 2^{a+1} \). Burnside (in [6]) has shown that if every element commutes with its conjugates, and \( 3 \not| g \), then \( G' \leq Z \); here if \( x \in K_i \) such that \( C(K_i) = C(x) \) then \( yxy^{-1} \in yC(K_i)y^{-1} = C(K_i) \), and because \( G \) cannot be abelian, then \( G' = Z \).

Hirsch [18] has shown that \( k \equiv g \pmod 3 \) for a 2-group. Since \( g = 2(k-1) = 2k-2 \), then \( k \equiv 2k - 2 \pmod 3 \) or \( k \equiv 2 \pmod 3 \). Hence \( g \equiv 2 \pmod 3 \) and since \( 2^2 \equiv 1 \pmod 3 \), the power of 2 which is \( g \) must be an odd power.
Let $x_2, x_3, \ldots, x_{2n+1}$ satisfy the relations: (i) the commutators not equal to 1 are exactly those of the form $[x_i, x_{2n+3-i}]$ $(2 \leq i \leq n+1)$ and are all equal to some $x_1$ which commutes with all $x_i$, $1 \leq i \leq 2n+1$; (ii) $x_i^2 = 1$; (iii) $x_i^2 = x_1$ for $2 \leq i \leq 2n$; (iv) either $x_{2n+1} = 1$ or $x_{2n+1} = x_1$. Both of the groups generated by the independent elements $x_2, x_3, \ldots, x_{2n+1}$ under the above relations have commutator subgroup $G' = \langle x_1 \rangle$ and center $Z = \langle x_1 \rangle$, from the defining relations above; both groups have order $2^{2n+1}$ since, modulo $Z$, they are elementary abelian groups with $2n$ generators and hence, modulo $Z$, have order $2^{2n}$ while $|Z| = 2$. In both groups every element is, of course, a product of powers of the generators, and the square of every element being in $Z$ then means that every element can be written uniquely as $x_1^{e_1}x_2^{e_2}\cdots x_{2n+1}^{e_{2n+1}}$ where each $e_i$ is 1 or 0. Let $y$ be an element not in $Z$ and let $j$ be the smallest integer such that $j \geq 2$ and $e_j \neq 0$ in the expansion of $y$. Form $x_{2n+3-j}(y)x_{2n+3-j}^{-1} = \prod_{i=1}^{j-1} x_{2n+3-i} x_1^{e_1} x_{2n+3-j}^{-1} = x_1^{e_1}(x_j^{e_j}x_1)x_{j+1}^{e_{j+1}} \cdots x_{2n+1}^{e_{2n+1}} = yx_1$. Since $K(y)$ is the set of all $x^{-1}yx = y[yx] \leq yG'$ which has order 2, then $|K(y)| = 2$ if $y \notin Z$. Therefore in (1.1.2) we have $g = h_1 + \cdots + h_k = 1 + 1 + 2 + 2 + \cdots + 2 = 2 + (k-2)(2) = 2(k-1)$ and we have established that both the above groups satisfy the conditions of (2.2.35).

Q.E.D.
Note that for \( n = 1 \) and \( n = 2 \), the groups defined above in the proof of (2.2.35) are the only ones to satisfy \( m_k = k-1 \), \( m_2 = 2(k-1) \) (see Hall and Senior [15]). Also compare with the results in section 2.3, for \( n = 1 \) (\( k = 5 \)).

Finally we wish to show that if \( 1 < t < k-1 \) in (2.2.33) no groups can have the corresponding class equation

\[
(2.2.36) \quad \frac{1}{y(k-1)} + \frac{1}{ty} + \frac{k-2}{k-1} = 1.
\]

To do this we need the following series of theorems. Note that \( |Z| = 1 \), because \( |Z| \neq 1 \) implies \( |Z| = 2 \) (otherwise \( m_3 \), and hence all \( m_1 \), equals \( g \)) and then \( m_2 = g \), which by (2.2.32) gives \( m_2 = 2(k-1) \), already done.

(2.2.37) Theorem: If prime \( p \mid y \) in (2.2.36) then \( p \mid (k-1) \).

Proof: If \( p \mid y \) and \( \exp K_2 \neq p \) then \( p \) must be the exponent of some \( K_j \), \( j > 2 \), because \( p \mid g \), and therefore \( p \mid m_j = k-1 \).

On the other hand, suppose \( \exp K_2 = p \), and \( K_2 = K(x) \). If \( t \) is a power of \( p \) we are done because \( t \mid (k-1) \) by (2.2.33).

Suppose then that some prime \( q \), distinct from \( p \), divides \( t \) and hence an element \( y \) of order \( q \) commutes with \( x \). Then \( x \in C(y) = C(K_j) \) for some \( j > 2 \), and so \( p \mid m_j = (k-1) \).

Q.E.D.

(2.2.38) Corollary: If prime \( p \mid y \) in (2.2.36), \( p \mid t \).

Proof: \( (y, \frac{k-1}{t}) = 1 \) by (2.2.33).

Q.E.D.
(2.2.39) **Theorem:** In (2.2.36), $y = p^a$ (p prime, $a \in J^+$), $\exp K_2 = p$, and $p^b \mid g$ implies $p^b \mid m_2$.

**Proof:** From (2.2.38) and (2.2.37), the highest power $p^b$ of a prime ply which divides $g$ must divide $m_2$ and no $m_i$ for $i > 2$. Now an element of order $p$ in the center of a $p$-Sylow subgroup of $G$ has centralizer of order divisible by $p^b$; therefore it must be in $K_2$, so $\exp K_2 = p$. As this must be true for all primes ply, then $y = p^a$, $a \in J^+$.

Q.E.D.

(2.2.40) **Corollary:** The class equation (2.2.36) becomes

\[
\frac{1}{p^a(p^a-1)t} + \frac{1}{p^{at}} + \frac{1}{(p^a-1)t} + \ldots + \frac{1}{(p^a-1)t} = 1
\]

where $p^a t$, p prime, $p^a \neq 2$.

(2.2.41) **Definitions:** If $x \in G$, we call $C(x)$ a fundamental subgroup (following Scorza [30], Chapter 4). If for all $y$, $G \neq C(x) \leq C(y)$ implies $C(y)$ is $C(x)$ or $G$, then $C(x)$ is a maximal fundamental subgroup.

Similarly, if for all $y$, $C(x) \supset C(y)$ implies equality, then $C(x)$ is a minimal fundamental subgroup.

A fundamental subgroup which is both maximal and minimal is free (Ito [20]).

The following two theorems are generalizations of theorems of Brauer and Fowler [5] and of Ito [20].
(2.2.42) **Theorem:** If $H$ is a maximal fundamental subgroup of $G$, then $H$ is abelian if and only if $H$ is the centralizer of every element of $H - Z(G)$, and both imply that if a prime $p^o(H)$ and $p \not| o(Z(G))$ where $p^{a|l|g}$, then $p^{a|l|o(H)}$.

**Proof:** Obviously if $H$ is abelian, $x \in H - Z, Z = Z(G)$, then $H \subseteq C(x)$, and by its maximality, then $H = C(x)$ or $G = C(x)$, the latter impossible since $x \not\in Z$. Conversely, if for every $x \in H - Z, H = C(x)$ then for all $x \in H, x \in Z(H)$ and so $H$ is abelian. Let $H$ be abelian, and let $p^o(H), p \not| o(Z)$, and $p^{a|l|g}$. If $y$ is an element of a $p$-Sylow subgroup of $H$, then $y$ commutes with the elements in the center of some $p$-Sylow subgroup $S_p$ of $G$. Therefore $Z(S_p) \subseteq C(y) = H$. If $x \in Z(S_p) \subset H$, then $S_p \subset C(x)$. But $x \in H, x \not\in Z$ since $x$ has order a power of $p$ and $p \not| o(Z)$, and $H$ is the centralizer of every element of $H - Z$. Therefore $H = C(x) \supseteq S_p$.

Q.E.D.

(2.2.43) **Theorem:** If $H$ is a minimal fundamental subgroup which is the centralizer of some element of prime power order $p^a$, then $H$ is nilpotent and the only Sylow subgroup of $H$ which can be non-abelian is that corresponding to $p$. 
Proof: Let $y \in H, |y| = n, (n,p) = 1$. Now $xy$ has order $p^an$ if $x$ is the element of $H$ with order $p^a$ and $H = C(x)$, because $x$ commutes with all elements of $H$. Take $s \in J$ such that $sn \equiv 1 \pmod{p}$. $C(xy) \leq C((xy)^{sn}) = C((x^{sn})(y^{ns})) = C(x) = H$ using (2.2.1) and that $x$ and $y$ commute. Since $H$ is minimal, then $xy \in Z(H)$. But then $y = (x^{-1})(xy) \in Z(H)$ since $x$, and so $x^{-1}$, is in $Z(H)$. It follows then that $|H/Z(H)|$ is a power of $p$, so $H/Z(H)$ is nilpotent and therefore $H$ is. The rest has already been shown.

Q.E.D.

(2.2.44) Theorem: If $H$ is a maximal fundamental subgroup then there exists some element $x$ of prime power order such that $H = C(x)$

Proof: Suppose every element of prime power order in $Z(H)$ is in $Z(G)$. Then every Sylow subgroup of $Z(H)$ must be in $Z(G)$ so $Z(H) \leq Z(G)$, a contradiction. Let $x \in Z(H) - Z(G)$ be of prime power order. Then $H \leq C(x) \not\subseteq G$ and therefore $H = C(x)$ by maximality.

Q.E.D.

(2.2.45) Theorem: If $H$ is a free fundamental subgroup of $G$ and $(|H|, |Z|) = 1$, then $H$ is abelian or a $p$-group.
Proof: Suppose \( H \) is a free fundamental subgroup of \( G \) of composite order. By (2.2.43) and (2.2.44) there is an element \( x \) of prime power order \( p^a \) in \( H \) so that \( H = C(x) \), and there is an element \( y \) of prime power order \( q^b \), \( q \neq p \), in \( Z(H) \). Since \( (|H|, |Z(H)|) = 1 \), then \( H \leq C(y) \neq G \) and so \( H = C(y) \). Applying (2.2.43) again, for \( y \), \( H \) must be nilpotent with all Sylow subgroups abelian, and hence \( H \) must be abelian.

Q.E.D.

(2.2.46) Theorem: No group has a class equation with \( m_k = k-1 \), and \( m_2 \) not equal to \( k \) or \( 2(k-1) \).

Proof: If such a group existed, we have seen that its class equation would satisfy (2.2.40). Since no \( C(K_i) \) has order dividing \( |C(K_j)| \neq g \) if \( i \neq j \) (because \((p^a t, (p^a-1)t) = t < (p^a-1)t\)) unless these orders are equal, then the fundamental subgroups of \( G \) must be free. Furthermore, since \( p^it \) and \((p^a-1) \neq 1 \), then \((p^a-1)t\) is composite. From \( Z(G) = 1 \), and (2.2.45), it follows that the fundamental subgroups of order \((p^a-1)t\) are abelian, and hence must be Hall subgroups (that is, their order and index are relatively prime) by (2.2.42). But by (2.2.39) the highest power of \( p \) divides \( m_2 \) and not \((p^a-1)t\), which, since \( p^it \), leads to a contradiction.

Q.E.D.
In (2.2.8) we saw that $2 \leq m_k \leq k-1$. In (2.2.7), (2.2.34), (2.2.35), and (2.2.46) we have looked at the extreme cases. For $m_k = 2$ the answer was simple and the proof straightforward; for $m_k = k-1$ we had much greater difficulty. One of the remarks made in section 2.5 is that for $k \leq 7$, the complexity of the groups seems to grow as $m_k$ approaches its mean possible value, $(k+1)/2$. If we wish to obtain general results, valid for all $k$, we will have to examine the cases of $m_k$ near its extremes first, and particularly $m_k = 3$ and $m_k = 4$ which promise, by the remarks above, to be easier than if $m_k = k-2$ or $k-3$. The ground has been broken already, for $m_k = 3$ by a paper of Feit and Thompson [11], and for $m_k = 4$ by Suzuki (see [33] and [34]); but such works are quite general, and rarely applicable to the approach of section 2.4.

In section 2.4 we will examine the class equation (1.1.4) for solutions, beginning with the minimum values of $m_k$, $m_{k-1}$, ... Thus, we consider $m_k = 2$ first, which is easy by (2.2.7), then the next case is that of $m_k = m_{k-1} = 3$. We know, of course, that $G$ is then $F(3,b)$ by (2.2.5). Since the regular subgroup $B$ is nilpotent, the problem reduces, in the main, to that of $p$-groups for $B$, using (2.2.6) and the following theorem.
(2.2.47) **Theorem:** If \( G \) is a direct product, \( G = H_1 \times H_2 \times \cdots \times H_n \), then for \( y_1 \in H_1 \), \( K_G(y_1 y_2 \cdots y_n) = \{ x_1 \cdots x_n \mid x_i \in K_{H_i}(y_i) \} \) and hence \( k(G) = k(H_1) \cdot k(H_2) \cdots k(H_n) \).

**Proof:** Denote \( \{ x_1 x_2 \cdots x_n \mid x_i \in K_{H_i}(y_i) \} \) by \( T \). Let \( a \in G \) and \( a = a_1 \cdots a_n \) in the direct factorization. By the definition of direct product \( a_i \) and \( y_j \) commute if \( i \neq j \), so \((a_1 \cdots a_n)(y_1 \cdots y_n)(a_1 \cdots a_n)^{-1} = a_1 y_1 a_1^{-1} \cdots a_n y_n a_n^{-1} \in T \).

On the other hand, if \( b_1, y_1 \in H_1 \), so that \( b_1 y_1 b_1^{-1} \in K_{H_1}(y_i) \) \((i = 1, \ldots, n)\), then again, \( b_1 y_1 b_1^{-1} \cdots b_n y_n b_n^{-1} = (b_1 \cdots b_n)(y_1 \cdots y_n)(b_1 \cdots b_n)^{-1} \in K_G(y_1 \cdots y_n) \).

Q.E.D.

Given \( k(G) \), \( g \) is bounded, and for a \( p \)-group, \( g = p^a \), the complexity of \( G \) increases more rapidly with \( a \) than with \( p \). Thus it is that in the case of \( m_k = m_{k-1} = 3 \), \( G = F(3, 2^a) \) causes the greatest difficulty. In the following theorems ((2.2.48) to (2.2.54)) we make some inroads on this problem. Recall from section 1.2 that \( G \) has elements of order 3 which act as \( \text{FPFA} \) (fixed-point-free automorphisms) of the regular subgroup \( B \).

(2.2.48) **Theorem:** Let \( G \) be an abelian 2-group with a \( \text{FPFA} \) \( t \) of order 3. If \( G = \langle x_1, \ldots, x_n \mid x_i^2 = 1 \rangle \) and if \( \langle x_1, \ldots, x_{n-2} \rangle \) is fixed under \( t \), then \( t: x_{n-1} \rightarrow x_n \rightarrow x_{n-1} x_n \). If \( G = \langle x, y \mid x^4 = y^4 = 1, [x, y] = 1 \rangle \) then \( t: x \rightarrow y \rightarrow x^3 y^3 \).
Proof: In both cases we simply apply the notion that
\( t: x \rightarrow y \rightarrow z \rightarrow x \) implies \( t: x y z \rightarrow y z x = x y z \) and so
\( x y z = 1 \) or \( z = x^{-1} y^{-1} \). Note that the action of \( t \) is
uniquely defined, up to the choice of generators.

Q.E.D.

(2.2.49) Theorem: If \( t \) is a FPFA of \( G \), then it induces a
FPFA of the same order on the factor group of
every characteristic subgroup of \( G \).

Proof: Let \( H \) be a characteristic subgroup of \( G \). Suppose
\( t \) does not induce a FPFA of order \( |t| \) on \( G/H \); say, \( t^a \)
leaves \( xH \) fixed for some \( x \not\in H \), and \( a \not\equiv 0 \pmod{|t|} \). But
then \( t^a \) permutes the elements of \( xH \) in sets of \( b \) with no
elements fixed, where \( b \) is the smallest divisor of \( |t| \) such
that \( o(t) \) \mid \( ab \). Therefore \( b \mid o(xH) = o(H) \). But \( b \mid o(t) \),
so \( b \mid o(H)-1 \), a contradiction.

Q.E.D.

(2.2.50) Theorem: Every group possessing a FPFA of order 3
is metabelian and if \( g = 2^a \) then \( 2 \mid a \).

Proof: \( G \) is metabelian (that is, \( G' \leq Z \)) by a theorem of
Neumann [27]. Because \( 3 \mid (g-1) = (2^a-1) \), \( a \) must be even.

Q.E.D.
(2.2.51) **Theorem:** If \( G \) is an abelian 2-group of type
\[
(n_1, n_2, \ldots, n_r),
\]
possessing a FPFA \( t \) of order 3,
and \( a \in J^+ \), \( s(a) = \) the number of distinct values
of \( i \) for which \( n_i = a \), then \( s(a) \equiv 0 \pmod{2} \).

**Proof:** Proof is by induction on \( g \). The theorem is true for
\( g = 4 \) since the cyclic group of order 4 has a group of auto-
morphisms of order 2, not 3, by (2.2.10), so \( G \) has type
\( (1,1) \). Now let
\[
G = \langle x_1, \ldots, x_r \mid x_1^{2^{n_1}} = 1, [x_i, x_j] = 1 \rangle.
\]
\[
\langle x_1^{2^{n_1}-1}, \ldots, x_r^{2^{n_r}-1} \rangle = G(2)
\]
has exponent 2 and is the
group generated by all elements of \( G \) of order 2. Thus \( G(2) \)
is characteristic and of type \( (1^r) \), while \( G/G(2) \) is
abelian of type \( (n_1-1, \ldots, n_r-1) \). But \( G/G(2) \) has a FPFA of
order 3 induced by \( t \) by (2.2.49); therefore \( G/G(2) \) satisfies
the conditions of (2.2.51). By the induction assumption
then \( s(a-1) \equiv 0 \pmod{2} \) over \( G/G(2) \), if \( a \neq 1 \), and hence
over \( G \) \( s(a) \equiv 0 \pmod{2} \). Since
\[
n_1 + n_2 + \cdots + n_r = \log_2(g) \equiv 0 \pmod{2}
\]
by (2.2.50), then the case \( s(1) \)
follows immediately.

Q.E.D.

(2.2.52) **Theorem:** If \( G = F(3, 2^a) \) then the regular sub-
group \( B \) of order \( b = 2^{2a} \) has \( k(B) \geq 5 \cdot 2^{a-1} - 1 = 5 \cdot 2^a - 1 \), with equality only if \( Z(B) \neq B' \),
provided \( B \) is non-abelian of course.
Proof: Let \( Z = Z(B) \) and note that \( B, Z, B', \) and their factor groups \( B/Z \) and \( B/B' \) are 2-groups possessing FPFA's of order three by (2.2.49), while \( B' \leq Z \) by (2.2.50).

Suppose \( |Z| = 2^a \). Every element \( x \) of \( B - Z \) has centralizer containing \( Z \) and \( x \) so \( |C_B(x)| \geq 2^{a+1} \) here, and \( |K_B(x)| \leq b/2^{a+1} = 2^{a-1} \). \( B - Z \) is divided into at least \( (b - 2^a)/2^{a-1} = 2(2^a - 1) \) classes over \( B \). Therefore \( k(B) \geq 2(2^a - 1) + |Z| = 3\sqrt[3]{2} - 2 \).

Suppose now \( |Z| > 2^a \), say \( |Z| = 2^a + h \) \((h \in J^+)\); then \( B/Z \) is abelian of order \( 2^{a-h} \) and by (2.2.29), \( k(B) \geq |Z| + [k(B/Z) - 1] = 2^{a+h} + 2^{a-h} - 1 \geq 2^{a+1} + 2^{a-1} - 1 = 5\sqrt[3]{2} - 1 \), since the value of \( 2^{a+h} + 2^{a-h} - 1 \) is monotonic decreasing as \( h \) decreases, provided \( h \leq a-2 \) which it is since \( |B/Z| \geq 4 \) by (2.2.50). Finally if \( |Z| < 2^a \), say \( |Z| = 2^a - h \) \((h \in J^+)\), then \( B/Z \) is abelian of order \( 2^{a-h} \) and again, by (2.2.29), \( k(B) \geq 2^{a-h} + (2^{a+h} - 1) \geq 5\sqrt[3]{2} - 1 \), using \( |Z| \neq 1 \) for a 2-group, and (2.2.50).

Q.E.D.

(2.2.53) Theorem: There are no non-abelian 2-groups of order less than 64 which possess a FPFA of order 3.

Proof: We can use (2.2.50) and the fact that every group of order 4 is abelian to reduce our examination to the case \( g = 16 \). \( G \) is metabelian by (2.2.50) so \( Z \geq G' \). Since both
are characteristic subgroups of $G$, then the FPFA $t$ of $G$
induces a FPFA of order 3 on $Z$, $G'$, $G/Z$, and $G/G'$ by (2.2.49)
and therefore by (2.2.50) and (2.2.51) these must all be
elementary abelian subgroups of order 4. Consulting
Burnside's listing of groups of order 16 ([7], p.146),
only numbers (iii) to (vi) are possible. But in all these
cases, the center $Z$ contains the square of a generator $x$
(denoted by $P$ in Burnside), and no two images of $x$ have
squares equal to the other two non-trivial elements forming
$Z$. Therefore it is impossible to take a FPFA of order 3 of
$G$ which will leave $Z$ fixed.

Q.E.D.

(2.2.54) Theorem: There are exactly two non-abelian 2-groups
of order 64 and possessing a FPFA of order 3 (say, $t$):

(1) $\langle x_1, \ldots, x_6 \rangle | x_1^2 = x_2^2 = x_5^2 = x_6^2 = 1, x_3^2 = x_1,$
    $x_4^2 = x_2,$ and non-trivial commutators $[x_3, x_5] = x_1,$
    $[x_4, x_5] = [x_3, x_6] = x_1x_2,$ $[x_4, x_6] = x_2 >$, with $t$:
    $x_1 \rightarrow x_2 \rightarrow x_1x_2,$ $x_3 \rightarrow x_4 \rightarrow x_1x_2x_3x_4,$
    $x_5 \rightarrow x_6 \rightarrow x_5x_6$;

(2) $\langle x_1, \ldots, x_6 \rangle | x_1^2 = x_2^2 = 1, x_3^2 = x_1,$
    $x_4^2 = x_5^2 = x_2,$ $x_6^2 = x_1x_2,$ and non-trivial commutators $[x_3, x_5] = x_1,$
    $[x_4, x_5] = [x_3, x_6] = x_1x_2,$ $[x_4, x_6] = x_2 >$, with $t$:
    $x_1 \rightarrow x_2 \rightarrow x_1x_2,$ $x_3 \rightarrow x_4 \rightarrow x_1x_2x_3x_4,$
    $x_5 \rightarrow x_6 \rightarrow x_5x_6$. 
Proof: Again we present a simple but non-constructive proof.

(For a constructive proof, we could use a modified form of theorem 3.5 of Hall and Senior [15]; by part (iii) of theorem 1.5 of Blackburn [2] and (2.2.51), \( G/G' \) must be abelian type (14) and \( G' = Z \) of type (1,1). Putting \( G_i = G/\langle u_i \rangle, \ u_i \in Z \), then all \( G_i \) (by \( t \)) must be of the same structure, either \( T_2 \) or \( T_5 \), Hall and Senior [15] notation. Now take up theorem 3.5 of Hall and Senior.)

We examine the list of 267 groups of order 64 in Hall and Senior [15], discarding those not having class 2 and \( |G'| = |Z| = 4 \), and then eliminating from the remainder those with characteristic subgroups of order 2 or 3, by (2.2.49) and (2.2.50). Only the family \( T_{13}^1 \) remains.

Of the five groups of \( T_{13}^1 \), only \( T_{13a_1}^1 \) and \( T_{13a_5}^1 \) have no characteristic subgroup of order 8. Their defining relations are presented in the statement of (2.2.54).

We now require the defining relations of \( t \), if they exist. \( T_{13a_1}^1 \) has only two normal subgroups of order 16 - 
\[ H = \langle x_1, x_2, x_5, x_6 \rangle \] and 
\[ \Pi = \langle x_1, x_2, x_3 x_5, x_4 x_6 \rangle \] - both of abelian type (1d). Since there are only two they must be fixed under \( t \). Since \( Z = \langle x_1, x_2 \rangle \) is fixed under \( t \), then by (2.2.48) we have \( t: x_5 \rightarrow x_6 \rightarrow x_5 x_6 \) and \( x_3 x_5 \rightarrow x_4 x_6 \rightarrow x_3 x_5 x_4 x_6 = x_1 x_2 x_3 x_4 x_5 x_6 \) so \( x_3 \rightarrow x_4 \rightarrow x_1 x_2 x_3 x_4 \).
Similarly in $\mathcal{A}_{13}$, there are five normal subgroups of order 16, abelian of type $(2,2)$, and because $o(t) = 3 \not= 5$, they all must be fixed under $t$. Two such groups are $\langle x_3, x_4 \rangle$ and $\langle x_5, x_6 \rangle$; by (2.2.48) $t: x_3 \rightarrow x_4 \rightarrow x_3 x_4^3 = x_1 x_2 x_3 x_4$ and $x_5 \rightarrow x_6 \rightarrow x_5 x_6^3 = x_1 x_5 x_6$.

Q.E.D.

This completes our investigation of the case $m_k = m_{k-1} = 3, \ G = F(3, 2^a)$. A similar result to (2.2.51) is the following theorem, also needed in section 2.4.

(2.2.55) Theorem: If $G$ is an elementary abelian 2-group possessing an automorphism $t$ of order 2, then $t$ leaves some subgroup $H$ of order not less than $\sqrt{g}$ elementwise fixed and is fixed-point-free over $G - H$.

Proof: Let $H = \{ y \in G \mid t(y) = y \}$. Then $H$ is a subgroup of $G$ since $t(y) = y$ and $t(y') = y'$ implies $t(yy') = t(y) \cdot t(y') = yy'$. Now let $x \in G - H$. Then $t(x) \in \langle x, H \rangle$, for if $t(x) = x'$, then since $|t| = 2$, $t(xx') = x'x = xx'$, so $xx' \in H$ or $x' \in x^{-1}H = xH$ since $|x| = 2$. Therefore for every element $x$ of $G - H$, $t(x) = xy$ where $y$ is some element of $H$. If $t(x) = xy$ and $t(x) = xy$, $y \in H$, then $t(xx) = xyxy = xxyy^2 = xx$ and so $x \in xH$, and conversely. Therefore there can be no more cosets of $H$ in $G$ than elements in $H$. That is, $|H| \geq \sqrt{g}$.  

Q.E.D.
The case of $m_k = 4$ is even more difficult. To begin, we mention two results on the 2-Sylow subgroups of $G$, obtained by Suzuki (see [33] and [34] respectively). The term semi-dihedral means $\langle x, y \mid x^{2n} = y^2 = 1, x^y = x^{-1+2n-1} \rangle$ (after Wong [37]).

(2.2.56) Theorem: If $m_1 = 4$ and $\exp K_1 = 2$, then the 2-Sylow subgroup $S_2$ of $G$ is dihedral of order $\geq 4$, or semi-dihedral of order $\geq 16$.

(2.2.57) Theorem: If $m_1 = 4$ and $\exp K_1 = 4$, then the 2-Sylow subgroup $S_2$ of $G$ must have a cyclic subgroup of index 2 and be one of: (i) cyclic of order 4, (ii) dihedral of order 8, (iii) quaternion of order $\geq 8$, (iv) semi-dihedral of order $\geq 16$.

In connection with these results we prove:

(2.2.58) Theorem: If $G = \langle x, y \mid x^{p^{n-1}} = y^p = 1, x^y = x^{1+p^{n-2}} \rangle$ then $k(G) = p^{n-1} + p^{n-2} - p^{n-3}$. If $G$ is a non-abelian group of order $p^n$ having a cyclic subgroup of index $p$, and not defined as above, then $p = 2$, $G$ is quaternion, dihedral, or semi-dihedral, and $k(G) = 2^{n-2} + 3$ with $m_1 = m_2 = g$, $m_k = m_{k-1} = 4$, and $m_1 = g/2$ if $2 < i < k-1$. 
Proof: Suppose $G = \langle x, y \mid x^{p^n-1} = y^p = 1, xy = x^{1+p^n-2}\rangle$.

Now (i) $x^{-1}(xy)^b x = x^{a-1}(yb) = x^{a-1}(x[l+p^n-2]b)y = x^{a+b}p^n-2yb$, and (ii) $y(xy)^b y^{-1} = (xa[l+p^n-2]y)y^{-1} = x^{a+ap^n-2}y$. Therefore $K(x^ayb) = \{xs(a,b)^p, x^ayb \mid \text{all } s \in J\}$.

It follows that $x^ayb \in Z$ if and only if $b \equiv 0 \pmod{p}$ by (i), and similarly for $a$ by (ii) since $x^{p^n-1} = 1$. Thus $Z = \langle x^p \rangle$ and $|Z| = p^{n-2}$. If $x^ayb \in G - Z$, then two conjugates are equal if and only if $xs(a,b)^p = xs(a,b)^p$ or $s(a,b) \equiv t(a,b)$ modulo $p$. Therefore the conjugates of $x^ayb$

can be generated by at most $p$ distinct values of $s$, modulo $p$; that is, $|K(x^ayb)| \leq p$. Since $x^ayb \not\in Z$, the $p^n - p^{n-2}$
elements of $G - Z$ are partitioned into $(p^n - p^{n-2})/p = p^{n-1} - p^{n-3}$ conjugate sets of $p$ elements each. Thus $k(G) = p^{n-2} + (p^{n-1} - p^{n-3})$.

Suppose now $G$ is quaternion $\langle x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, x^y = x^{-1} \rangle$ or dihedral $\langle x, y \mid x^{2^{n-1}} = y^2 = 1, xy = x^{-1} \rangle$. In each of these two cases, $G = \langle x^ayb \mid a = 1, \ldots, 2^{n-1}, b = 1, 2 \rangle$, and $Z = \langle x^{2^{n-2}} \rangle$, $|Z| = 2$, and $x^n(x^ay)x^{-r} = x^{a+2r}y$, $y(xy)^{-1} = yx^a = x^{-ay}$. Obviously $C_G(x^a \in G - Z) = \langle x \rangle$ so $|K(x^a)| = 2$ and there must be $(2^{n-1} - 2)/2 = 2^{n-2} - 1$ such conjugate sets. Since, for $1 \leq a \leq 2^{n-1}$, $K(x^ay) = \{xs(a^22r)^p \mid \text{all } s \in J\}$ must have order $2^{n-2}$, the $2^{n-1}$ elements of the form $x^ay$ split into two classes. Therefore $k(G) = (2^{n-2} - 1) + 2 + 2 = 2^{n-2} + 3$. 
If $G$ is semi-dihedral $\langle x, y \mid x^{2n-1} = y^2 = 1, \ yxy^{-1} = x^{-1}x^{2n-2}\rangle$, then again $Z = \langle x^{2n-2}\rangle$ so that the elements of the form $x^a$ fall into 2 conjugate sets of 1 element each, namely $\{x^{2n-2}\}$ and $\{x^{2n-1}=1\}$, and $2n-2 - 1$ classes of two elements each. Here, $x^r(x^ay)x^{-r} = x^{a+r}(yx^{-r}) = x^{a+r}(x^{r+2n-2}y)$ and $y(x^ay)y^{-1} = yxa = x^{-a+a2n-2}y$; hence $K(x^ay) \geq \{x^{a+s}y \mid \text{all } s \in J_p^2 + \{x^{a+2+2n-2}y\}$ so that its order is strictly greater than $2n-1/4 = g/8$, and since $|Z| = 2$ the centralizer of any element $x^ay$ must have order at least 4. Therefore $|K(x^ay)| = 2n-2$ and so again we have $k(G) = 2n-2 + 3$.

By Burnside ([7], p.135) these four groups are the only non-abelian $p$-groups with a cyclic subgroup of index $p$. In the last three cases, we had two $m_1 = g$ from $Z$, two $m_1 = 4$, and the remaining $m_1 = g/2$. Since $G$ is non-abelian and of order $2^n$, $g \geq 8$ and (2.2.58) now follows from (1.1.5).

Q.E.D.

We also need a generalization of (2.2.5).

(2.2.59) Theorem: If for $p^{a-1}$ distinct values of $i$, $m_i = p^a$, and $p^a \mid g$, then $G$ is $F(p^a, g/p^a)$. The converse is true if $p$ is odd.
Proof: The proof runs similarly to that of (2.2.5). If \( m_1 = p^a \) for \( p^a - 1 \) values of \( i \), then the number of solutions of \( x^{p^a} = 1 \) is at least \( 1 + (p^a - 1)(g/p^a) \). Let \( n \) be the number of \( p \)-Sylow subgroups \( S_p \) of \( G \); there are at most \( 1 + n(p^a - 1) \) elements of order a power of \( p \), and since \( p^a \lvert G \), then \( n \geq g/p^a \). Now \( n \cdot |N_G(S_p)| = g \) (Burnside [7], p.151). Therefore \( N_G(S_p) = S_p \), \( n = g/p^a \), and the intersection of distinct \( p \)-Sylow subgroups is trivial. By the Theorem of Frobenius \( G \) must be \( F(p^a, g/p^a) \).

Conversely, if \( G \) is \( F(p^a, g/p^a) \) then \( p^a \lvert G \) since \( (p^a, g/p^a) = 1 \), and if \( p \) is odd, then the complementary subgroup is a cyclic \( p \)-Sylow subgroup \( \langle x \rangle \) of \( G \) (Burnside [7], p.335). Since \( G \) is a Frobenius group, then \( K(x^c) \neq K(x^d) \) if \( c \not\equiv d \pmod{p^a} \) and \( G(x^c) = \langle x \rangle \) if \( c \not\equiv 0 \pmod{p^a} \). It follows that \( m_1 = p^a \) for \( p^a - 1 \) distinct values of \( i \).

Q.E.D.

(2.2.60) Theorem: If \( m_k = m_{k-1} = m_{k-2} = 4 \), then \( 8 \lvert G \), or \( G = F(4, 4k-15) \) and \( m_1 = 4k-15 \) if \( 1 < i < k-2 \).

Proof: First we note that by (2.2.56) and (2.2.57) the only possibility for the \( 2 \)-Sylow subgroup \( S_2 \) of \( G \) if \( 16 \lvert G \) is semi-dihedral, and by (2.2.58), \( m_k = m_{k-1} = m_{k-2} = 4 \) is impossible over \( S_2 \) and even more so over \( G \). Therefore \( |S_2| \leq 8 \). Suppose \( |S_2| = 4 \). By (2.2.59), \( G \) is \( F(4, g/4) \). The
regular subgroup \( B \) must be abelian since the complementary subgroup \( S_2 \) has order 4 (Burnside [7], p.172). Therefore by (2.2.6) \( k = 4 + (b-1)/4 \) and \( b = 4k - 15 \). If \( x \neq 1 \), \( x \in G - (K_k + K_{k-1} + K_{k-2}) = G - (\cup S_2 - 1) = B \), then \( C_G(x) = B \), so \( m_1 = b = 4k - 15 \) for \( 1 < i < k-2 \). Note that \( S_2 \) must be cyclic here (Burnside [7], p.335).

Q.E.D.

There is some difficulty in proving that such groups \( F(4,4k-15) \) exist for all \( k \geq 5 \). For example, by the results of section 2.3, the regular subgroup is not necessarily cyclic, as in (2.2.7). It may be that the Sylow subgroups of \( B \) must be elementary abelian, but the defining relations for the corresponding PPFA of order 4 are unknown.

(2.2.61) Theorem: If \( m_k = m_{k-1} = m_{k-2} = 4 \), \( m_1 = 8 \), then \( G \) is the quaternion or dihedral group of order 8, so \( k = 5 \) and \( m_1 = m_2 = 8 \), or \( G \) is \( F(8,8k-39) \), \( i = k-3 \), and \( m_j = 8k-39 \) if \( 1 < j < k-3 \).

Proof: By (2.2.60), \( 811g \), and by (2.2.56) and (2.2.57), the 2-Sylow subgroups of \( G \) are quaternion or dihedral. If \( g = 8 \), we are done by (2.2.58). Otherwise, there are \( 1 + g/8 + 3(g/4) = 1 + 7(g/8) \) solutions of \( x^8 = 1 \) at least, so the number of 2-Sylow subgroups \( S_2 \) must be at least \( g/8 \) and by Burnside ([7], p.151), \( N_G(S_2) = S_2 \), again giving by
the Theorem of Frobenius, $G = \mathbb{F}(8, g/8)$. The regular subgroup $B$ is abelian (Burnside [7], p.172) and has order $8k - 39$ by (2.2.6), and the non-trivial elements not in $K_k$, $K_{k-1}$, $K_{k-2}$, or $K_1$, are in $B$ and so have centralizers of order $8k - 39 > 8$.

Therefore by (1.1.5), $i = k - 3$. Note that here $S_2$ must be quaternion (Burnside [7], p.335) and $B$ must be the direct product of two isomorphic abelian groups (Wong [38]).

Q.E.D.

Also useful in this case is a theorem of Brauer and Fowler [5]:

(2.2.62) Theorem: Let $x \in G$ such that $x^{-1} \in K(x)$ and $1 \neq y \in C(x)$ implies $C(y) = C(x)$. Let $v$ be the number of elements of $G$ of order 2, and $n = g/v$. If $|C(x)| = c > n$, then $g \leq c(c-2)n/(c-n)$.

(2.2.63) Theorem: If for an odd number of values of $i$ $m_i = p$ (prime), then $G$ contains an element $x$ of order $p$ satisfying (2.2.62).

Proof: Suppose for every element $x$ of order $p$, $x^{-1} \notin K(x)$. Then $K(x^{-1}) = \{y^{-1} : y \in K(x)\}$, since $zx^{-1} = y$ if and only if $z(x^{-1})z^{-1} = (zxz^{-1})^{-1} = y^{-1}$. Let $s$ be the number of classes of exponent $p$. It is impossible that $s = 1$, since $x^{-1}$ has order $p$ as $x$ does, and we supposed $x^{-1} \notin K(x)$. 

Suppose we have counted off an even number of classes of exponent $p$, taking $K(x^{-1})$ with $K(x)$. Let $|z| = p$, $K(z)$ not counted. Then $K(z^{-1})$ is not counted either, for if it were, as $K(x)$, then $K(x^{-1}) = \{y^{-1} \mid y \in K(x)\}$, containing $z$, would have been counted too. Hence by induction, $s$ is even. But by (2.2.4) this contradicts that for an odd number of values of $i$, $m_i = p$. Therefore there exists some $x \in G$ of order $p$ with $x^{-1} \in K(x)$. But by (2.2.4) then $|C(x)| = p$ and therefore $1 \notin y \in C(x)$ implies $y = x^a$, $(a,p) = 1$, which implies by (2.2.1) $C(y) = C(x)$.

Q.E.D.

If $|K_i| = |K_{i+1}| = g/4$ and $\exp K_i = \exp K_{i+1} = 2$ then combining (2.2.62) and (2.2.63) gives:

(2.2.64) **Theorem:** If for two distinct values of $i$, $m_i = 4$ and $\exp K_i = 2$, then the number of $m_j = p$ (prime) is even.

(2.2.65) **Theorem:** If $m_i = 4$, $\exp K_i = 2$, and $m_j = p$ (prime) for an odd number of distinct values of $j$, then $p = 3$, or $G = \text{Alt}(5)$, or $G = F(4,p)$ and for three distinct values of $i$, $m_i = 4$. 

Proof: Using (2.2.62) and (2.2.63), \( g \leq \frac{p(p-2)^4}{p-4} \) if \( p > 4 \).

But for \( p > 5 \), \( \frac{p-2}{p-4} < 2 \) and so \( g < 8p \). Since \( 4p \mid g \), \( g = 4p \). The number of \( p \)-Sylow subgroups of \( G \) is congruent to 1 modulo \( p \) and is also a divisor of \( g/p \) (Burnside [7], p.151).

Since \( 4 < p \), there can be only one \( p \)-Sylow subgroup \( S_p \). By (2.2.4) every element of \( G \) has order dividing \( p \) or \( g/p = 4 \).

By a theorem of Feit [10], \( G = F(4,p) \). The elements not in the regular subgroup of \( G \) have centralizers of order \( m_1 = 4 \), and since there are \( g/p = 3p \) such elements, and since \( |K_1| = p \), there must be 3 such \( m_1 = 4 \).

Finally if \( p = 5 \), then \( g \leq 5 \cdot 3 \cdot 4/1 = 60 \); since \( 20 \mid g \), then \( g = 20, 40, \) or \( 60 \). \( |G| = 20 \) gives \( G = F(4,5) \) by exactly the same argument as above; and \( g = 60 \) and some \( m_j = p = 5 \) means there are at least \( h_j = 12 \) elements of order 5, and hence \( G \) has no normal 5-Sylow subgroup.

Burnside ([7], p.161) has shown that \( G = \text{Alt}(5) \) under these conditions. If \( g = 40 \), then \( m_j = 5 \) means \( G \) has no normal 5-Sylow subgroup again. But the number of 5-Sylow subgroups divides \( g = 40 \) and is congruent to 1 modulo 5. It follows that there is no such group of order 40.

Q.E.D.
We conclude with a few theorems which are very restricted, easily proved, but useful.

(2.2.66) Theorem: If \( m_1 = 4 \) and \( 2^b \mid \ell \), \( b \geq 2 \), then \( G \) contains elements of orders \( 2^{b-1}, 2^{b-2}, \ldots, 4, \) and 2 whose centralizers have order divisible by \( 2^{b-1} \).

Proof: Let \( |S_2| = 2^b \). By (2.2.56) and (2.2.57), \( S_2 \) (and so \( G \)) contains an element \( x \) of order \( 2^{b-1} \); \( x^2 \) has order \( 2^{b-2} \), and so on, and since \( C(x) \leq C(x^a) \) by (2.2.1), then \( 2^{b-1} \) divides the order of \( C(x^a) \) for any \( a \).

Q.E.D.

(2.2.67) Theorem: If a group \( B \) of order \( b = p_1^{a_1} \cdots p_n^{a_n} \) (its prime decomposition) possesses a FPF of order \( r \), then \( r \) divides \( (b-1), (p_1^{a_1} - 1) \), and \( \lambda(S_{p_i})! - 1 \) for the \( p_i \)-Sylow subgroup \( S_{p_i} \) of \( B \), for all \( i \).

Proof: See my M.Sc. thesis [28].

Q.E.D.
(2.2.68) **Theorem**: Let $i < 4$. Suppose $(m_j, m_1) = 1$ and $m_j$ is a prime power for every $j > i$. If $	ext{exp } K_i = p$ (prime), $p-1$ composite with some prime dividing $p-1$ which does not divide $m_i$, then $\text{exp } K_i' = p$ for some $i' < i$. In particular, if $m_i = p$ (prime), $p-1$ composite, then $m_i' = p$ for some $i' < i$.

**Proof**: Suppose for only $i' = i$ does $\text{exp } K_i' = p$. Then by (2.2.11), $G$ contains an element of order $p-1$ and some class $K_a$ for it. Since $m_j$ is not composite for $j > i$, then $a < i$. Hence at most two classes have index which is composite and divisible by a prime not dividing $m_i$, contradicting (2.2.16). Q.E.D.

(2.2.69) **Theorem**: If in addition to the conditions of (2.2.68), $(p-1)/2$ is composite or a prime power $q^b$ such that $\text{exp } K_j = q^c$ implies $c < b-1$ ($j > i$), then for three values of $i^*$, $\text{exp } K_{i^*} = p$.

**Proof**: If for only two values of $i^*$, $\text{exp } K_{i^*} = p$, then $p^{(p-1)/2}$ is the order of an element of $G$ by (2.2.11). There is at most one class whose exponent is not assigned yet. If $(p-1)/2$ is composite, we contradict (2.2.16), and if $(p-1)/2 = q^b$, then there must be elements of order $q^b$, $q^{b-1}$, and so on in $G$, again contradicting the given conditions. Q.E.D.
(2.2.70) **Theorem:** The number of solutions of $x^n = 1$, $n \mid g$, in $G$ is a multiple of $n$. Suppose $pq \mid m_i$ if and only if $i \in T < J$, $p$ and $q$ primes, $p \neq q$, and if $j \notin T$, $p \nmid m_j$. Then for some non-empty proper subset $S$ of $T$, $p \mid \left( \sum_{i \in S} h_i + 1 \right)$.

**Proof:** The first statement is well-known (Burnside [7], p.52). Since $p$ is a prime, the number of solutions of $x^p = 1$ is one more than the number of elements in classes of exponent $p$. We are given that $\exp K_i = p$ only if $i \in T$ so we are left only to prove that $S$ is non-empty and proper, in $T$. If $S$ were empty, then $p \mid 1$; if $S = T$, then we contradict (2.2.16). Q.E.D.

(2.2.71) **Theorem:** If $G$ contains exactly $b$ solutions of $x^b = 1$, some $m_1 = b$, and $(m_j, b) \neq 1$ implies $m_j = b$, for any $j$, then $G = F(g/b, b)$.

**Proof:** Since $(m_j, b) \neq 1$ implies $m_j = b$ for all $j$, then every element of $G$ has order dividing $b$ or $g/b$. Since $m_1 = b$, then $G$ contains a subgroup $B$ of order $b$, which is then the set of all elements of order dividing $b$, and hence characteristic. By a theorem of Feit [10], $G = F(g/b, b)$. Q.E.D.
Section 2.3: A List Of Groups With $k(G) \leq 7$.

The following, up to and including the case $k = 5$, is a reproduction of the list given by Burnside in [8] of all group class equations, together with the groups that have such a class equation, as given, again for $k \leq 5$, by Miller [23]. I extend this for the cases $k = 6$ and $k = 7$.

In attempting to find any previous articles on this, I discovered (very recently) one by Sigley [32], which made no reference to previous work, other than that of Miller for $k \leq 5$ already cited. As no reference is made to this problem in the review journals (Math.Zentralblatt and Math.Reviews) in the years 1935 - 1965, I will assume this article by Sigley is the only one examining $k = 6$ and $|\mathbb{Z}| = 1$, and $k = 7$ and $|\mathbb{Z}| = 2$. In comparing his results with mine (our methods differ) I found that he had omitted the case $k = 6$ and $g = 72$. In the section of his work where this result should have appeared, he presents no proofs. I hope to avoid any such errors by giving a detailed proof in section 2.4.

Excluding Alt(n) and Sym(n) which are well-known, I will state the generating relations of each group corresponding to the given class equation.
\[(2.3.1) \quad \frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1\]

for \(G = F(2, 3) = \text{Sym}(2)\).

\[(2.3.2) \quad \frac{1}{10} + \frac{1}{5} + \frac{1}{5} + \frac{1}{2} = 1\]

for \(G = F(2, 5) = \langle x, y \mid x^5 = y^2 = 1, xy = x^4 \rangle\).

\[(2.3.3) \quad \frac{1}{12} + \frac{1}{4} + \frac{1}{3} + \frac{1}{3} = 1\]

for \(G = F(3, 4) = \text{Alt}(4)\).

\[(2.3.4) \quad \frac{1}{14} + \frac{1}{7} + \frac{1}{7} + \frac{1}{2} = 1\]

for \(G = F(2, 7) = \langle x, y \mid x^7 = y^2 = 1, xy = x^6 \rangle\).

\[(2.3.5) \quad \frac{1}{21} + \frac{1}{7} + \frac{1}{7} + \frac{1}{3} = 1\]

for \(G = F(3, 7) = \langle x, y \mid x^7 = y^3 = 1, xy = x^2 \rangle\).

\[(2.3.6) \quad \frac{1}{24} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4} + \frac{1}{3} = 1\]

for \(G = \text{Sym}(4)\).

\[(2.3.7) \quad \frac{1}{60} + \frac{1}{5} + \frac{1}{5} + \frac{1}{4} + \frac{1}{3} = 1\]

for \(G = \text{Alt}(5)\).

\[(2.3.8) \quad \frac{1}{8} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1\]

for Quaternion \(\langle x, y \mid x^2 = y^2, x^4 = 1, xy = x^3 \rangle\)
and Dihedral \(\langle x, y \mid x^4 = y^2, xy = x^3 \rangle\).

\[(2.3.9) \quad \frac{1}{20} + \frac{1}{5} + \frac{1}{4} + \frac{1}{4} = 1\]

for \(G = F(4, 5) = \langle x, y \mid x^5 = y^4 = 1, xy = x^2 \rangle\).
(2.3.10) \[ \frac{1}{18} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{2} = 1 \]

for \( F(2,9) = \langle x, y \mid x^9 = y^2 = 1, xy = x^8 \rangle \)
or \( F(2,9) = \langle x, y, z \mid x^3 = y^3 = z^2 = 1, xy = x, x^2 = x^2, y^2 = y^2 \rangle \).

(2.3.11) \[ \frac{1}{168} + \frac{1}{8} + \frac{1}{7} + \frac{1}{4} + \frac{1}{3} = 1 \]

for \( LF(2,7) = \langle x, y \mid x^7 = y^2 = (xy)^3 = (x^4y)^4 = 1 \rangle \).

(2.3.12) \[ \frac{1}{36} + \frac{1}{9} + \frac{1}{9} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1 \]

for \( F(4,9) = \langle x, y, z \mid x^4 = y^3 = z^2 = 1, x^2 = y, y^2 = y, z^2 = y^2 \rangle \).

(2.3.13) \[ \frac{1}{72} + \frac{1}{6} + \frac{1}{4} + \frac{1}{4} = 1 \]

for \( F(8,9) = \langle w, x, y, z \mid w^4 = x^4 = y^3 = z^3 = 1, w^2 = x^2, x^w = x^3, y^z = y, y^w = z, z^w = y^2, y^x = yz, z^x = yz^2 \rangle \).

(2.3.14) \[ \frac{1}{12} + \frac{1}{12} + \frac{1}{6} + \frac{1}{4} + \frac{1}{4} = 1 \]

for \( \langle x, y \mid x^3 = y^4 = 1, xy = x^2 \rangle \)
or \( \langle x, y, z \mid x^3 = y^2 = z^2 = 1, x^2 = x^2, x^y = x, y^2 = y \rangle \).

(2.3.15) \[ \frac{1}{22} + \frac{1}{11} + \frac{1}{11} + \frac{1}{11} + \frac{1}{2} = 1 \]

for \( F(2,11) = \langle x, y \mid x^{11} = y^2 = 1, xy = x^{10} \rangle \).

(2.3.16) \[ \frac{1}{39} + \frac{1}{13} + \frac{1}{13} + \frac{1}{13} + \frac{1}{3} + \frac{1}{3} = 1 \]

for \( F(3,13) = \langle x, y \mid x^{13} = y^3 = 1, xy = x^3 \rangle \).
(2.3.17) \[ \frac{1}{52} + \frac{1}{13} + \frac{1}{13} + \frac{1}{13} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1 \]

for \( F(4,13) = \langle x, y \mid x^{13} = y^4 = 1, xy = x^5 \rangle \).

(2.3.18) \[ \frac{1}{16} + \frac{1}{16} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1 \]

for Dihedral \( \langle x, y \mid x^8 = y^2 = 1, xy = x^7 \rangle \)
or Semi-Dihedral \( \langle x, y \mid x^8 = y^2 = 1, xy = x^3 \rangle \)
or Quaternion \( \langle x, y \mid x^8 = 1, x^4 = y^2, xy = x^7 \rangle \).

(2.3.19) \[ \frac{1}{126} + \frac{1}{12} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{4} + \frac{1}{4} = 1 \]

for Sym(5).

(2.3.20) \[ \frac{1}{360} + \frac{1}{9} + \frac{1}{9} + \frac{1}{8} + \frac{1}{5} + \frac{1}{5} + \frac{1}{4} = 1 \]

for Alt(6).

(2.3.21) \[ \frac{1}{24} + \frac{1}{24} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{4} = 1 \]

for \( \langle x, y, z \mid x^2 = y^2, x^4 = z^3 = 1, xy = x^3, x^2 = y, y^2 = xy \rangle \).

(2.3.22) \[ \frac{1}{55} + \frac{1}{11} + \frac{1}{11} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5} = 1 \]

for \( F(5,11) = \langle x, y \mid x^{11} = y^5 = 1, xy = x^4 \rangle \).

(2.3.23) \[ \frac{1}{42} + \frac{1}{7} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = 1 \]

for \( F(6,7) = \langle x, y \mid x^7 = y^6 = 1, xy = x^3 \rangle \).
Section 2.4: Proof.

We will not show that the groups presented in section 2.3 actually exist or have the class equations indicated; this process is very straightforward. We will attempt to show that for \( k = 6 \) and \( k = 7 \) no other groups can have a given class equation and that no other solutions of (1.1.4) can be group class equations. To establish the latter, we will show that any group having such an equation for its class equation would involve a contradiction. Much of this work has been done in section 2.2.

We proceed by examining successive, increasing values of \( m_k \), with the corresponding possible values of \( m_{k-1} \), then \( m_{k-2} \), and so on. In order to calculate \( m_j \) when we have taken values for \( m_{j+1}, \ldots, m_k \), we use an inequality, derived by Landau's method (see section 1.1).

\( (2.4.1) \) Notation: Let \( t_j = \text{LCM} \{m_1 \mid 1 > j\} \); \( s_j = \frac{1}{m_{j+1}} + \cdots + \frac{1}{m_k} \)

for \( j = 0, 1, \ldots, k-1 \).

\( (2.4.2) \) Theorem: \( \frac{1}{1-s_j} \leq m_j \leq \frac{(j-1)t_j + (m_j, t_j)}{(1-s_j)t_j} \leq \frac{1}{1-s_j} \)

for \( 2 \leq j \leq k-1 \); in particular, \( m_2 = \frac{t_2 + (m_2, t_2)}{(1-s_2)t_2} \).
Proof: Substituting (2.4.1) in (1.1.4), we have

\[
1 = \frac{1}{t_1} + (\frac{1}{m_2} + \cdots + \frac{1}{m_j}) + s_j \leq \frac{1}{t_1} + (\frac{1}{m_j} + \cdots + \frac{1}{m_j}) + s_j
\]

\[
\leq \frac{1}{t_{j-1}} + \frac{j-1}{m_j} + s_j = \frac{(m_j, t_j)}{m_j \cdot t_j} + \frac{j-1}{m_j} + s_j, \quad \text{for } 2 \leq j \leq k-1
\]

with equality throughout in the case \( j = 2 \). Therefore

\[
m_j \cdot t_j \leq (m_j, t_j) + (j-1)t_j + s_j t_j m_j \quad \text{or} \quad m_j \leq \frac{(j-1)t_j + (m_j, t_j)}{(1-s_j)t_j}
\]

which has a maximum value of

\[
\frac{(j-1)t_j + t_j}{(1-s_j)t_j} = \frac{j}{(1-s_j)}. \quad \text{Q.E.D.}
\]

(2.4.3) Corollary: \( m_j = \frac{(j-1)t_j + (m_j, t_j)}{(1-s_j)t_j} \) implies \( m_2 = m_j \).

The value of \( m_1 \) will always be chosen as \( t_1 \). Thus \( s_0 \neq 1 \) will mean that with the given \( m_1 \) (\( i \geq 1 \)) and the corresponding \( m_1 = t_1 \), the sum of all \( 1/m_i \) (\( 1 \leq i \leq k \)) is not unity as is necessary in (1.1.4). At some points as well, the sum of the \( 1/m_i \) for \( i \) greater than some \( j \) may be more than 1 --- that is, \( s_j > 1 \) --- and therefore \( s_0 > s_j > 1 \) and again (1.1.4) cannot be satisfied. In most cases we will use (2.4.2) and (1.1.5) without explicit reference. To indicate that no groups exist with order and class number equal to given values \( g \) and \( k \), we refer just to the list of all groups \( G \) of order \( g \); the calculation of \( k(G) \) is then straightforward.
Case (1). $m_6 = 2$.

We obtain (2.3.10) immediately from (2.2.7). Since the order $b$ of the regular subgroup $B$ is 9, $B$ is cyclic -- and hence we have the first group stated in (2.3.10) -- or $B$ is elementary abelian $\langle y_1, y_2 \rangle$, in which case either $x: y_1 \rightarrow y_2$ (but $y_1 y_2 \neq 1$ fixed) or $x: y_1 \rightarrow y_1^{-1}, y_2 \rightarrow y_2^{-1}$, giving the second group.

Case (2). $m_6 = m_5 = 3$.

$G$ is $F(3,b)$ by (2.2.5), and by (2.2.6), $k(B) = 10$ for the regular subgroup $B$. $B$ cannot be abelian because of (2.2.67). $B$ is nilpotent and the direct product of its Sylow subgroups. But if $B$ is not a p-group, then by (2.2.47) it is the product of p-groups of class numbers 2 and 5; the former is for a group of order 2 by (2.2.9), contradicting (2.2.67). Hence $B$ is a p-group, and since $k(B)$ is even, so is $b$ by (2.2.19). Therefore $B$ is a 2-group. By (2.2.52), $t \leq \left[\frac{2}{5}(10+1)\right]^2 < 20$ and by (2.2.53), $B$ must be abelian, which we have discarded.
Case (3). \( m_5 = 3, m_5 \neq 3 \).

By (2.2.4), \((m_5, t_5) = (m_5, 3) = 1 \) so in (2.4.2), \( m_5 \leq 13/2 \).

Again by (2.2.4), \( m_5 = 4 \) or 5 only.

(1) If \( m_5 = 5 \) then \( m_2 \neq 5 \) (otherwise \( s_1 > 1 \)) and therefore by (2.2.13), \( m_3 \neq 5 \). If \( m_4 = 5 \), \((m_3, t_3) = (m_3, 15) = 1 \) and \( m_3 \leq 31/4 \), so \( m_3 = 7 \) by (2.2.4). But then \( m_2 = 7 \) by (2.2.15) so \( g \) is odd contradicting (2.2.19). It follows that \( m_4 \neq 5 \); but then \((m_4, t_4) = 1 \) and \( m_4 < 7 \), contradicting (2.2.4).

(ii) If \( m_5 = 4 \), then \( m_3 \neq 4 \) (otherwise \( s_2 > 1 \)). If \( m_4 = 4 \), then \( 6 < m_3 \leq 14 \) using \((m_4, t_4) \leq 4 \). The values 14 and 10 can be discarded by (2.2.16); 12 and 9 by (2.2.4); the primes 13 and 11 by (2.2.69), and 7 by (2.2.15) and \( s_1 > 1 \). Thus \( m_3 = 8 \), so \( m_2 = 25, 26, 28, \) or 32 using \((m_2, t_2) = 1, 2, 4, \) and 8 respectively. The first implies \( G = F(24, 25) \) by (2.2.71), with a complementary subgroup of order 24 and class number 5 (by (2.2.6)) and 2-Sylow subgroup cyclic or quaternion (Burnside [7], p.335), but no such group exists (see (2.3.6)); \( m_2 = 26 \) and \( m_2 = 28 \) are out by (2.2.16); \( m_2 = 32 \) contradicts (2.2.66).

If \( m_5 = 4 \) and \( m_4 \neq 4 \), then \( m_4 \leq 8 \) using \((m_4, t_4) \leq 4 \) so \( m_4 = 5, 7, \) or 8 by (2.2.4). If \( m_4 = 8 \), \( m_2 = 8 \) and \( g = 24 \) by (2.4.3), but no group of order 24 has class number 6 (Burnside [7], section 126). If \( m_4 = 7 \), \( m_3 = 7 \) by (2.2.15)
and \(m_2 = 8\) is the only integral value, with \((m_2, t_2) = 4\).

By (2.2.20) and the values of the \(h_1\) here, \(G\) must be simple and it is well-known (Burnside [7], Note N) that \(G\) is \(LF(2, 7)\) giving (2.3.11). Finally if \(m_4 = 5\), then \(m_3 < 10\) so \(m_3 = 5, 7\), or \(8\) by (2.2.4). For \(m_3 = 8, m_2 = 11\) with \((m_2, t_2) = 1\) for \(m_2\) integral, and this contradicts (2.2.68); for \(m_3 = 7, m_2 = 7\) by (2.2.15) so \(s_1 > 1\); for \(m_3 = 5, m_2 = 61, 62, \) or \(64\) taking \((m_2, t_2) = 1, 2, \) or \(4\) respectively. The first is impossible by (2.2.63), the second by (2.2.16), and the last by (2.2.66).

**Case (4).** \(m_0 = m_5 = m_4 = 4\).

By (2.2.60), if \(G\) is not \(F(4, 9)\), then \(8| s_2\), so \(8\) divides some \(m_1\), and if \(m_1 = 8\) (so \(i = 3\) by (2.2.61)) then we have (2.3.13) exactly and its group by (2.2.61). The case \(8p \mid m_3\) instead, for \(p\) some odd prime, is impossible by (2.2.16). Therefore \(G = F(4, 9)\) and since the cyclic group of order 9 has an automorphism group of order 6 (by (2.2.10)) while the group of order 9 here must have a FPFA of order 4, then \(S\) must be elementary abelian and (2.3.12) follows.
Case (5). \( m_6 = m_5 = 4, m_4 \neq 4. \)

Therefore \( m_4 \leq 8, \) and if \( m_4 = 8, g = 8 \) which cannot be (Burnside [7], p.146) for \( k = 6. \) The case \( m_4 = 7 \) is impossible since \( s_0 < 1/28 + 3/7 + 2/4 < 1. \)

If \( m_4 = 6, \) then 6 divides \( (m_3, t_3) \) and \( (m_2, t_2) \) by (2.2.16) and as \( m_3 < 12 \) then \( m_3 = 6. \) Hence \( m_2 = 12 \) with \( (m_2, t_2) = 12 \) in order that \( 6m_2, \) so \( g = 12 \) and the two groups of (2.3.14) follow from Burnside [7], section 59.

If \( m_4 = 5, \) then \( m_3 < 7 \) for \( (m_3, t_3) = 1, \) and \( m_3 < 8 \) otherwise, so \( m_3 = 6 \) or 5, with the former excluded by (2.2.16).

If \( m_3 = 5, \) then \( m_2 = 12 \) for \( m_2/(m_2, t_2) \in J; \) this contradicts (2.2.16).

Case (6). \( m_6 = 4, m_5 \neq 4. \)

Therefore \( m_5 \leq 6, \) and \( m_5 = 6 \) implies \( m_2 = 6 \) by (2.4.3) so \( g = 12, |Z| = 1, \) which would mean \( G = Alt(4), k(G) = 4 \) (Burnside [7], section 59). Thus \( m_5 = 5, \) and so \( m_4 \leq 6 \) or \( m_4 = 5. \) Then \( m_3 < 7 \) with \( m_3 = 6 \) eliminated by (2.2.16), while \( m_3 = 5 \) gives \( m_2 = 5 \) by (2.2.13) and then \( s_1 > 1. \)

Case (7). \( m_6 = 5. \)

By (2.2.46), \( m_2 = 6 \) or 10, and the latter is impossible by (2.2.35). Also \( m_2 = 6 \) is impossible, for then \( G = F(5, 5) \) and so 5 divides 3-1 and 2-1 by (2.2.67).
\[ k = 7 : \quad 2 \leq m_7 \leq 6 \quad \text{by (2.2.8)}. \]

**Case (1).** \( m_7 = 2 \).

By (2.2.7), \( G = F(2,11) \) and the regular subgroup of order 11 must be cyclic so the only possibility is (2.3.15).

**Case (2).** \( m_7 = m_6 = 3 \).

By (2.2.5), \( G \) is \( F(3,b) \) with \( k(B) = 13 \) for the regular subgroup \( B \), by (2.2.6). If \( B \) is abelian, then it is cyclic of order 13 and we have (2.3.16). By (2.2.47), \( B \) must be a \( p \)-group. Since \( 3 \mid [o(Z(B)) - 1] = p^n - 1 < 13 \) by (2.2.67), then \( p^n = 4 \) or 7. If \( B \) is a 7-group, then \( k(B/Z) \geq \mid Z(B/Z) \mid > 7 \) by Burnside [7], p.120. By (2.2.29), \( k(B) \geq 7 + 14 - 1 = 20 \), a contradiction. If \( B \) is a 2-group, \( |Z(B)| = 4 \), then \( b \leq \frac{2}{5}(13+1) < 36 \) by (2.2.52), and by (2.2.53) \( B \) cannot be non-abelian.

**Case (3).** \( m_7 = 3 \), \( m_6 \neq 3 \).

Therefore \( m_6 \leq 8 \), with \( m_6 = 8 \) only if \( m_2 = 8 \) and \( \varepsilon = 24 \) by (2.4.3), and, again, no such group exists with \( k = 7 \) (Burnside [7], section 126). Only the values 4, 5, and 7 are possible for \( m_6 \) by (2.2.4).
(i) If $m_6 = 7$, then $m_5 = 7$ by (2.2.15) and $m_4 < 8$, with $m_4 = 8$ implying $m_2 = 8$ and $s = 168$. Now such a group has 64 solutions $(K_1 + K_2 + K_3 + K_4)$ of $x^8 = 1$ and therefore at least $63/7 = 9$ 2-Sylow subgroups $S_2$. By Burnside [7], p.151, there must be $21 S_2$, so distinct 2-Sylow subgroups intersect non-trivially. But $S_2$ is abelian ($2|m_1$ implies $8|m_4$) so (Burnside [7], p.154) some element of order a power of 2 must commute with an element of relatively prime order, meaning some $m_1$ composite, a contradiction. Therefore $m_4 = 7$; then $m_3 < 9$, and since $m_3 \neq 7$ by (2.2.13), then $m_3 = 8$. But no integral solution of (2.4.2) exists for $m_2$, taking $(m_2, t_2) / 8$.

(ii) If $m_6 = 5$, then $m_5 < 9$ so $m_5 = 5, 7, 8$. If $m_6 = 8$, then $m_4 < 9$ for $(m_4, t_4) \leq 8$. But $m_4 = 8$ means $m_3 < 10$ as above so $m_3 = 8$ by (2.2.4) and hence $m_2 = 11$ ($(m_2, t_2) > 1$ makes $m_2$ non-integral) contradicting (2.2.15). If $m_5 = 7$ then $m_4 = 7$ by (2.2.15) and $m_3 < 12$. By (2.2.4), $m_3 = 7, 8, 11$ and the latter is impossible by (2.2.15) and $s_0 \neq 1$, while the other two give non-integral values for $m_2$.

Finally if $m_5 = 5$, then $m_4 < 12$, so $m_4 = 5, 7, 8, 11$ by (2.2.4). For $m_4 = 11$, $m_3 = 11$ by (2.2.15) and then $m_2$ is non-integral; for $m_4 = 7$, $m_3 = 7$ by (2.2.15) so $s_2 > 1$; for $m_4 = 5$, $m_3 = 5$ by (2.2.13) and again $s_2 > 1$. Therefore
\( m_4 = 8, \) and \( m_3 < 15 \) so \( m_3 = 8, 11, 13, \) or \( 14 \) by (2.2.4).

Now \( m_3 = 14 \) is impossible by (2.2.16), \( m_3 = 13 \) by (2.2.69), and \( m_3 = 11 \) by (2.2.15) and \( s_0 \neq 1, \) and so \( m_3 = 8 \) and \( m_2 = 64 \) with \((m_2, t_2) = 8\) (otherwise \( m_2/(m_2, t_2) \notin \mathcal{J}\)).

By Burnside [7], Note \( N, G \) is not simple, but by (2.2.20) only \( N_{16} = K_1 + K_2 \) of order 16 can be normal in \( G, \) so \( G/N_{16} \simeq \text{Alt}(5). \) Take any two distinct 2-Sylow subgroups \( S_2 \) and \( S_2' \) in \( G. \) Obviously \( N_{16} \triangleleft S_2 \) and \( S_2', \) and \( N_{16} \) is elementary abelian by \( N_{16} = K_1 + K_2 \) containing some element of order 2. If \( y \in S_2 - N_{16}, \) then \( y^2 \in N_{16} \) because no element of \( \text{Alt}(5) \) has order 4. Since \( N_{16} \triangleleft S_2, \) \( y \) is an automorphism of an elementary abelian group and by (2.2.55) commutes with at least 4 elements of \( N_{16}. \) Thus \( \text{In}(C_{S_2}(y)) \).

But \( y \in K_3 + K_4, \) so \( |C_{S_2}(y)| \leq 8 \) and we have \( |C_{S_2}(y)| = 8. \) Therefore the 64 - 16 elements of \( S_2 - N_{16} \) fall into \( \frac{64-16}{8} = 6 \) classes of order \( 64/8 = 8 \) over \( S_2. \) By Hall and Senior [15] however, no group of order 64 has more than 5 classes of order 8.

(iii)If \( m_5 = 4 \) then \( m_5 < 10 \) if \((m_5, t_5) = 1, \) and \( m_5 \leq 10 \) if \((m_5, t_5) = 2, \) in which case, for \( m_5 = 10, m_2 = 10 \) and \( g = 60 \) by (2.4.3), contradicting (2.2.70) using \( p = 5. \) Therefore \( m_5 = 4, 5, 7, \) or \( 8 \) by (2.2.4).
If \( m_5 = 8 \), \( m_4 < 11 \) \((m_4, t_4) = 8 \) gives \( m_4 < 12 \) and so nothing new. So \( m_4 = 8 \) or 10 by (2.2.4). If \( m_4 = 10 \), \( m_3 < 11 \) so \( m_3 = 10 \), and then \( m_2 = 11 \) \((m_2, t_2) > 1 \) gives \( m_2 \not\in J \) contradicting (2.2.16); if \( m_4 = 8 \), \( m_3 < 14 \) and we can discard 9 and 12 by (2.2.4), 10 and 14 by (2.2.16), and 11 and 13 by (2.2.69). If \( m_3 = 8 \), \( m_2 = 25, 26, 28, \) or 32 for \((m_2, t_2) = 1, 2, 4, \) and 8 respectively; 26 and 28 we can exclude by (2.2.16), 32 by (2.2.66), and 25 because (2.2.71) makes \( G = F(24, 25) \) with complementary subgroup of order 24 and class number 6 (by (2.2.6)), contradicting section 2.3.

If \( m_5 = 7 \), \( m_4 = 7 \) by (2.2.15), so \( 7 < m_3 < 16 \) or \( m_3 = 8, 10, 11, \) or 13 by (2.2.4). For \( m_3 = 13 \) or 11, we contradict (2.2.69); for \( m_3 = 10 \), we contradict (2.2.16); hence \( m_3 = 8 \) and \( m_2 = 169, 170, 174, \) and 178 with \((m_2, t_2) = 1, 2, 4, \) and 8 respectively. The latter three are composite and excluded by (2.2.16), while \( m_2 = 169 \) means \( \exp K_2 = 13 \), contradicting (2.2.68).

If \( m_5 = 5 \), then \( m_4 < 14 \) or \( m_4 = 14 \) and \( m_2 = 14 \), \( g = 420 \) by (2.4.3), contradicting (2.2.70) with \( p = 7 \). Therefore \( m_4 = 5, 7, 8, 11, \) or 13 by (2.2.4). For \( m_4 = 13 \), \( m_2 = 13 \) by (2.2.69) and then \( s_1 > 1 \); for \( m_4 = 11, m_3 = 11 \) by (2.2.15) and then \( m_2 \not\in J \); for \( m_4 = 8, 8 < m_3 < 22 \), equality excluded by (2.2.16), so \( m_3 = 11, 13, 14, 16, 17, \) or 19 by (2.2.4).
and the primes \( \neq 11 \) are excluded by (2.2.69), while \( m_2 = 11 \) makes \( m_2 = 11 \) by (2.2.15) and \( s_0 \neq 1 \); \( m_3 = 14 \) contradicts (2.2.16); and \( m_3 = 16 \) gives \( m_2 \notin J \). For \( m_4 = 7 \), \( m_3 = 7 \) by (2.2.15), and then \( s_2 > 1 \). Finally, for \( m_4 = 5 \) we have

\[ 61 \leq m_3 \leq 121 \text{ if } (m_3, t_3) = 1, \quad 122 \text{ if } (m_3, t_3) = 2, \text{ or } 124 \text{ if } (m_3, t_3) = 4. \]

For \( m_3 = 121 \), \( m_2 = 121 \) by (2.4.3) and by (2.2.71) \( G = F(60, 121) \). The complementary subgroup of order 60 has class number 5 by (2.2.6), making it \( \text{Alt}(5) \) by (2.3.7), which has no element of order 4, contradicting Burnside [7], p.335. Otherwise \( m_3 \) cannot be composite by (2.2.16), and the only prime powers in this range are 64 (contradicting (2.2.66)), 121 (already dealt with), and primes themselves (contradicting (2.2.69)).

If \( m_5 = 4 \), then \( 6 < m_4 < 19 \text{ if } (m_5, t_5) = 1 \), with \( m_4 = 20 \) possible if \( (m_5, t_5) = 4 \), in which case \( m_2 = 20 \) and we contradict (2.2.70) for \( p = 5 \). Therefore \( m_4 = 7, 8, 10, 11, 13, 14, 16, \text{ or } 17 \) by (2.2.4). We can exclude 17 and 13 by (2.2.69) and \( s_1 > 1 \), and 11 and 7 by (2.2.68) and \( s_2 > 1 \).

If \( m_4 = 14 \), then by (2.2.16) \( 14 \mid (m_4, t_4) \) for \( i = 2, 3 \); and by \( m_3 < 25 \) then \( m_3 = 14 \), so \( m_2 = 56 \) with \( (m_2, t_2) = 28 \) (for 14, \( m_2/(m_2, t_2) \notin J \)), contradicting (2.2.70) for \( p = 7 \). If \( m_4 = 10 \), then by (2.2.15), \( 10 \mid (m_4, t_4) \) for \( i = 2, 3 \); and by \( 10 < m_3 \leq 35 \), then \( m_3 = 20 \) (excluding 30 by (2.2.4)) and \( m_2 = 70 \) (contradicting (2.2.16)) or 80 (contradicting (2.2.66)).
The case of \( m_4 = 16 \) is excluded by (2.2.66), so we reduce to \( m_4 = 8 \); then \( 24 < m_3 \leq 49, 50, 52, \) or \( 56 \) for \((m_3,t_3) = 1, 2, 4, \) and \( 8 \) respectively, the latter three rejected because of (2.2.16), and 49, by (2.4.3) and (2.2.71), giving \( G = F(24,49) \) with complementary subgroup of order 24, class number 5 (by (2.2.6)), and 2-Sylow subgroup cyclic or quaternion, against (2.3.6). Excluding by (2.2.4), (2.2.16), (2.2.69) and (2.2.66) as usual, we have \( m_3 = 25 \), so \( m_2 \) is 601, 602, 604, 605, 608, or 625 for \((m_2,t_2) = 1, 2, 4, 5, 8, \) or 25 (the only possible values by (2.2.16)). The prime 601 is impossible by (2.2.68), and the composite numbers 602, 604, 605, and 608 contradict (2.2.16), so \( m_2 = 625 \), and by (2.2.71) \( G = F(24,625) \). The complementary subgroup has order 24, class number 5 (by (2.2.6)), and is non-existent as above.

**Case (4).** \( m_7 = m_5 = m_5 = 4 \).

If \( 4 \mid t_2 \) then \( G = F(4,13) \) by (2.2.60), with the regular subgroup of order 13 obviously cyclic, giving (2.3.17).

Otherwise \( 8 \mid t_2 \). If some \( m_1 = 8 \), then by (2.2.61), \( G \) is \( F(8,17) \). But in this case there are two classes of elements of order 17, so by (2.2.13) \( G \) contains an element of order 8, contradicting (2.2.66).
If no $m_1 = 8$, then 8 divides some $m_1$ by $8l_1g$, so that $m_1$ is composite and by (2.2.16) $m_4$, $m_3$, $m_2$ each must be even composite numbers. Now $m_4 \leq 14$ and 16 for $(m_4, t_4) = 2$ and 4 so $m_4 = 6, 10, 12, \text{ or } 14$, the latter impossible by (2.4.3) and $8l_1g$. If $m_4 = 12$, then $12 \mid (m_3, t_3)$ and as $m_3 \leq 18$, $m_3 = 12$; again $12 \mid (m_2, t_2)$ so $m_2 \leq 24$ and $8l_1g$ gives $m_2 = 24$, which is impossible (Burnside [7], section 126). If $m_4 = 10$ then $10 \mid (m_3, t_3)$ so $m_3 < 14$ makes $m_3 = 10$; again $10 \mid (m_2, t_2)$ so $m_2 = 30$ or 40. The first is excluded by (2.2.16), and $m_2 = 40$ means, by (2.2.70) and (2.2.71), that $G = F(8, 5)$, contradicting (2.2.67). If $m_4 = 6$, then $6 \mid (m_3, t_3)$ so $12 < m_3 \leq 36$. Now $K_4$ must have elements of order 6 or 3, by $8l_1g$ and (2.2.16), so $3l_1g$. Therefore $m_3 = 24$ (excluding 30 by (2.2.16) as usual), and with $6 \mid (m_2, t_2)$ and $24 < m_2 \leq 48$, no value of $m_2$ satisfies $3l_1g$, $8l_1g$.

Case (5). $m_7 = m_6 = 4$, $m_5 \neq 4$.

Therefore $m_5 < 9$ with $(m_5, t_5) = 1$ (otherwise $m_5 \leq 9$ and 10 for $(m_5, t_5) = 2$ and 4) or $m_5 = 5, 6, 7, \text{ or } 8$.

(1) If $m_5 = 8$, then $m_4 < 9$ if $(m_4, t_4) \leq 2$ ($m_4 < 11$ otherwise), so $m_4 = 8$. Then $m_3 < 9$ if $(m_3, t_3) = 1$, and $m_3 \leq 9, 10, \text{ and } 12$ for $(m_3, t_3) = 2, 4, \text{ and } 8$ respectively, so $m_3 = 8$. Therefore $m_2 = 9, 10, 12, \text{ or } 16$ for $(m_2, t_2) = 1$,
2, 4, and 8 respectively. The first gives $G = F(8, 9)$ by (2.2.71) with complementary subgroup of order 8 and class number 6, contradicting section 2.3 results for $k = 6$; by (2.2.16) then $m_2 = 16$, $g = 16$, and from Burnside [7], p.146, (2.3.18) results.

(ii) If $m_5 = 7$, then $m_4 < 9$ so $m_4 = 7$ or 8, the latter not possible because of (2.2.14) and (2.2.16). Therefore $m_3 \leq 10$ with equality eliminated by (2.2.16). If $m_3 = 9$, $m_2 \notin J$; if $m_3 = 8$, then only $m_2 = 12$ is integral and this contradicts (2.2.16); if $m_3 = 7$, then $m_2 = 18$ for $m_2/(m_2, t_2) \notin J$, and this contradicts (2.2.66).

(iii) If $m_5 = 6$, then $m_4 < 11$ and $m_4 = 10$ contradicts (2.2.16) for 6 and 10. If $m_4 = 9$, then $6 | m_3$ by (2.2.16) so $9 \leq m_3 < 14$, with $m_3 < 11$ if $(m_3, t_3) \leq 12$, so $m_3$ can take on no value. If $m_4 = 8$, $6 | m_3$ again so $8 \leq m_3 < 15$ with $m_3 \leq 12$ if $(m_3, t_3) \leq 12$ and therefore $m_3 = m_2 = 12$, $g = 24$, by (2.4.3), and this is impossible (Burnside [7], section 126). If $m_4 = 7$, $6 | m_3$ again so $7 \leq m_3 < 12$ -- impossible. Finally for $m_4 = 6$, we note that if $6 \not| m_3$, then $6 | m_2$ by (2.2.16) but $36 \not| m_2$; indeed if it did, and $6 | \exp K_2$, then powers of elements in $K_2$ would be in other $K_1$ with $36 \not| m_1$ by (2.2.1), and otherwise, $\exp K_2 = 2$ say, then an element of order 3 must commute with one of order 2 and another element of
order 3, since $9 \mid g$, a contradiction too. Now $7 \leq m_3 < 13, 14, 14, 15, 16, \text{ and } 18 \text{ for } (m_3, t_3) = 1, 2, 3, 4, 6, \text{ and } 12$ and none of the latter adds any new values, so $m_3 = 7, 8, 9, \text{ or } 12, 10$ excluded by (2.2.16) and 11 by (2.2.69). If $m_3 = 7$, we must have, by the discussion above, $m_2 = 48$, which contradicts (2.2.66); if $m_3 = 8$, again we get $m_2 = 48$, or we can have $m_2 = 36$, which we excluded; if $m_3 = 9$, the only possible value is $m_2 = 24$, which, since $9 \mid g$, contradicts that some element of order 3 must commute with an element of order 2 (by (2.2.16)) and another element of order 3. Thus $m_3 = 12$, so $m_2 = 13, 14, 15, 16, 18, \text{ or } 24 \text{ for } (m_2, t_2) = 1, 2, 3, 4, 6, \text{ and } 12 \text{ respectively.}$ The values 14 and 15 are excluded by (2.2.16), 16 by (2.2.66), 18 because $x^9 = 1$ only if $x \in S_3 = Z(S_3)$ or $9 \mid o(C_0(x))$, giving only 3 solutions of $x^9 = 1$, against (2.2.70). By Burnside [7], section 126, 24 is excluded, and 13 is excluded since $\exp K_1 = 12$ by (2.2.14) means 12 divides the orders of the centralizers of the powers of the elements of $K_1$ by (2.2.1), not all of which will be in $K_1$.

(iv) If $m_5 = 5$, then $m_4 < 11$ if $(m_4, t_4) = 1$ and $m_4 < 12$ otherwise, so $m_4 = 5, 6, 7, 8, \text{ or } 9$. If $m_4 = 9, m_3 < 11$ and by (2.2.16) $m_3 = 9$, giving $m_2/(m_2, t_2) \not\in J$. If $m_4 = 8, m_3 < 13$; excluding by (2.2.4) and (2.2.16) we have $m_3 = 8$. 


9, or 11, and \( m_3 = 11 \) implies \( m_2 = 11 \) by (2.2.15) so \( s_1 > 1 \); 
\( m_3 = 9 \) gives only \( m_2 = 16 \) satisfying \( m_2/(m_2, t_2) \in J \) and this 
contradicts (2.2.66); \( m_3 = 8 \) gives only \( m_2 = 24 \) satisfying 
\( m_2/(m_2, t_2) \in J \) and this contradicts (2.2.16). If \( m_4 = 7, \) 
\( m_3 = 7 \) by (2.2.68), giving \( m_2 = 72 \) for \( m_2/(m_2, t_2) \in J \), which 
is excluded by (2.2.16). If \( m_4 = 6, \) then \( 7 < m_3 < 18 \) with 
\( 6 \mid m_3 \) and \( m_2 \) by (2.2.16), so \( m_3 = 12 \) and \( m_2 = 24 \). Then 8|g 
and since \( x \in Z(S_2) \) implies \( 8 \mid o(C(x)) \), then \( \exp K_2 = 2 \). If 
\( \exp K_3 = 6, \) then for some \( i, K_i = K(y^2), \) \( \exp K_1 = 3, \) 
and \( 12 \mid m_1 \) by (2.2.1), a contradiction. Therefore \( \exp K_3 = 3, \) 
\( \exp K_4 = 6 \) by (2.2.16), and \( o(K_1 + K_3) = 10 = o\{x : x^3 = 1\}, \) 
contradicting (2.2.70).

Case (6). \( m_7 = 4, \) \( m_6 \neq 4. \)

Then \( m_6 \leq 7 \) if \( (m_6, t_6) = 1 \) (equality excluded by 
(2.4.3) and (2.2.13)), and \( m_6 \leq 8 \) otherwise, giving \( g = 8, \) 
k = 7, impossible by Burnside [7], p.146. Therefore \( m_6 = 5 \) 
or \( 6. \)

(1) If \( m_6 = 6, \) then \( m_5 \leq 7 \) if \( (m_5, t_5) = 1 \) (equality again 
contradicting (2.2.13)), and \( m_5 \leq 8 \) and \( 9 \) for \( (m_5, t_5) \leq 6 \) 
and \( 12 \) respectively. Therefore \( m_5 = 6, \) and \( m_4 \leq 8 \) if 
\( (m_4, t_4) \leq 4 \) or \( m_4 < 10 \) otherwise. Now \( m_4 = 8 \) makes \( m_2 = 8 \) 
contradicting (2.2.16) for \( m_1 = 6, \) so \( m_4 = 6 \) or \( 7. \) For
\( m_4 = 7, \ m_3 < 8 \) so \( m_3 = 7 \), making \( m_2 = 8 \) for \( m_2/(m_2,t_2) \in J \), contradicting (2.2.16) again. Hence \( m_4 = 6, \) and \( m_3 < 9, 10, 11, \) and 13 for \( (m_3,t_3) \leq 2,3,6, \) and 12 respectively, with \( m_3 = 12 \) out by Burnside [7], section 59, \( m_3 = 10 \) out by (2.2.16), and \( m_3 = 9 \) out by \( x \in S_3 \) implies \( 9 \in \sigma(C(x)) \), contradicting (2.2.13) for \( m_1 = 6 \). If \( m_3 = 8, \ m_2 = 9 \) (not possible for the same reason) or 12, for \( m_2/(m_2,t_2) \in J \), and this latter is excluded by Burnside [7], section 126. If \( m_3 = 7, \ m_2/(m_2,t_2) \notin J \). Hence \( m_3 = 6 \) too, and then \( m_2 = 13, 14, 15, 16, 18, \) or 24 for \( (m_2,t_2) = 1,2,3,4,6, \) and 12 respectively; we reject 14 and 15 by (2.2.16), 13 by (2.2.66), 16 by (2.2.66), and 18 since \( x \in S_2 \) implies \( 4 \in \sigma(C(x)) \), against (2.2.16) for \( m_1 = 6 \). This leaves \( m_2 = 24 \) and by Burnside [7], section 126, we have (2.3.21).

(ii) If \( m_6 = 5, \) then \( m_5 < 8 \) so \( m_5 = 5, 6, \) or 7. If \( m_5 = 7 \) then \( m_4 < 8, \) so \( m_4 = 7, \) and \( m_3 < 8, \) so \( m_3 = 7, \) all of which gives \( m_2 \notin J \). If \( m_5 = 6, \) then \( m_4 \leq 8 \) for \( (m_4,t_4) \leq 4 \) and \( m_4 < 9 \) otherwise. Now \( m_4 = 8 \) gives \( m_2 = 8 \) by (2.4.3), contradicting (2.2.16) for \( m_1 = 6 \), while \( m_4 = 7 \) gives \( m_3 < 9, \) again, contradicting (2.2.16) for \( m_1 = 6 \). Therefore \( m_4 = 6 \) and \( m_3 < 10 \) if \( (m_3,t_3) \neq 12 \) (otherwise \( m_3 < 11 \)). If \( m_3 = 7 \) or 9, \( m_2 \notin J, \) so \( m_3 = 6 \) or 8. For \( m_3 = 6, \ m_2/(m_2,t_2) \notin J \) unless \( m_2 = 21 \) or 24. The first is excluded by (2.2.16) and
the second because $81_{lg}$ means $K_2 = \{x \in Z(S_2) \mid x^2 = 1\}$ and to satisfy (2.2.70), only one of $K_3$, $K_4$, and $K_5$ can have exponent 3. The other two must have exponent 6 or 2, and if both are of exponent 6, then $o(K_1 + K_2 + K_7) = 36 = o\{x \mid x^8 = 1\}$, contradicting (2.2.70). Therefore, say, \(\exp K_3 = 2\), \(\exp K_4 = 6\), and \(\exp K_5 = 3\). Since \(N_0(S_3)\) has a fixed structure, \(\exp K_2 = \exp K_3 = 2\) imply every element of order 3 commutes with two elements of order 2, contradicting \(\exp K_5 = 3\), \(m_5 = 6\).

This leaves \(m_3 = 8\), \(6 \mid m_2\) by (2.2.16), and, for \(m_2/(m_2, t_2) \in J\) too, \(m_2 = 12\), so \(g = 120\). The symmetric group satisfies these conditions (Scott [31], p.299), giving (2.3.19). No other group does; indeed, the normal subgroups of \(G\) can only have orders 40 and 60 by (2.2.20), and if \(G\) had a normal subgroup of order 40 it would be characteristically simple and hence (Burnside [7], p.92) the direct product of isomorphic simple groups. This is impossible since the only simple groups of order \(\leq 40\) are cyclic of prime order (Burnside [7], Note N) and 40 is not a power of a prime. Therefore \(G\) has a characteristically simple subgroup of order 60 and hence simple by the same argument, or \(G\) is simple which again is not possible. It follows that this simple group of order 60, the only normal subgroup of \(G\), is \(\text{Alt}(5)\) (Burnside [7], Note N), so \(G\) is \(\text{Sym}(5)\).
Finally for $m_5 = 5$, $m_4 < 9$ if $(m_4, t_4) \leq 10$ if $(m_4, t_4) = 4$.

Therefore $m_4 = 5$, 6, 7, or 8. If $m_4 = 5$, then $m_3 = 5$ by (2.2.13) and then $s_2 > 1$; if $m_4 = 6$, then $6 \mid m_3$ and since $m_3 \leq 12$, then $m_3 = 6$ or 12. Now $m_3 = 12$ means $m_2 = 12$ by (2.4.3) and by (2.2.16) and (2.2.70) we must have 5 elements of order 3, which is impossible since any two distinct 3-Sylow subgroups intersect trivially, giving an even number of elements of order 3. If $m_3 = 6$ on the other hand, then for $6 \mid m_2$ by (2.2.16), $m_2 = 66$ or 72, the former out by (2.2.16) and the latter because $81 \mid g$ and $91 \mid g$ imply $\exp K_2$ is 2 and 3 for $Z(S_2)$ and $Z(S_3)$. If $m_4 = 7$, then $m_3 = 7$ by (2.2.68), so $m_2 = 12$ for $m_2 \in J$; this contradicts (2.2.16).

Finally for $m_4 = 8$, $m_3 \leq 9$ if $(m_3, t_3) = 1$, and $m_3 < 10$ otherwise. If $m_3 = 9$, $m_2 = 9$ by (2.4.3); by (2.2.20) this group is simple, and by Note N of Burnside [7], $G = \mathrm{Alt}(6)$ and we have (2.3.20). If $m_3 = 8$, then $m_2 / (m_2, t_2) \notin J$.

Case (7). $m_7 = m_6 = m_5 = m_4 = 5$.

By (2.2.5), $G = F(5, b)$ and by (2.2.6), the regular subgroup $B$ has class number 11. Since $B$ is nilpotent, by (2.2.47) $B$ is a $p$-group, with $5 \mid [o(Z(B)) - 1] = p^a - 1 < 11$ by (2.2.67). Therefore $|Z(B)| = |B| = 11$ and $G$ is $F(5, 11)$, giving (2.3.22).
Case (8). \( m_7 = m_6 = m_5 = 5, m_4 \neq 5 \).

Impossible by (2.2.13).

Case (9). \( m_7 = m_6 = 5, m_5 \neq 5 \).

Then \( m_5 \leq 7 \), with equality giving \( m_2 = 7 \), contradicting (2.2.13). Thus \( m_5 = 6 \), and \( m_4 \leq 7 \) for \( m_4 \in J \); \( m_4 = 7 \) makes \( m_2 = 7 \), contradicting (2.2.16) for \( m_1 = 6 \). Therefore \( m_4 = 6 \), and \( m_3 < 8 \) or 9 for \( (m_3, t_3) \leq 3 \) and \( (m_3, t_3) = 6 \) respectively, so \( m_3 = 6 \) or 7, the latter giving \( m_2 \notin J \). For \( m_3 = 6 \), \( m_2 = 12 \) for \( m_2/(m_2, t_2) \in J \), and then since \( o(K_6 + K_7) = 25 - 1 = o\{x \mid x^5 = 1\} - 1 \), then by Burnside [7], section 127, \( G \) is Alt (5), contradicting (2.3.7).

Case (10). \( m_7 = 5, m_6 \neq 5 \).

Then \( m_6 < 7 \) so \( m_6 = 6 \); then \( m_5 < 7 \) so \( m_5 = 6 \); then \( m_4 < 7 \) so \( m_4 = 6 \); then \( m_3 < 7 \) if \( (m_3, t_3) = 1 \) and \( m_3 < 8 \) otherwise so \( m_3 = 6 \). Hence \( m_2 = 8 \) for \( m_2/(m_2, t_2) \in J \), and since \( \exists ! g \), then \( K_2 = \{x \in Z(S_2) \mid x^2 = 1, x \neq 1\} \). But then no \( K_1 \) has exponent 4 or 8, contradicting (2.2.14).

Case (11). \( m_7 = 6 \).

By (2.2.46) \( m_2 = 7 \) or 12, the latter impossible by (2.2.35). If \( m_2 = 7 \), \( G = F(6,7) \) by (2.2.34), giving (2.3.23).

This completes \( k = 7 \).
Section 2.5: Conjectures.

The most striking characteristic of the list of groups with class number \( k \leq 7 \), presented in section 2.3, is that the group with maximum order for a given value of \( k \) is simple. The three simple non-abelian groups of lowest order are \( \text{Alt}(5) \) of order 60, \( LF(2,7) \) of order 168, and \( \text{Alt}(6) \) of order 360 (Burnside [7], Note N). These are (2.3.7) with \( k = 5 \), (2.3.11) with \( k = 6 \), and (2.3.20) with \( k = 7 \), respectively, and every group with one of these class numbers has smaller order than the simple group with the same class number. Perhaps the least upper bound of the order of a finite group with at most \( k \) classes is the maximum of the orders of the simple groups with class number at most \( k \).

Actually the term "simple group" is ironic; simple groups have been the object of endless pursuit and have a structure which is at the opposite pole to abelian groups.

Consider the following classification of groups, drawn from M.Hall [14]: ① abelian, ② nilpotent but not abelian, ③ supersolvable but not nilpotent, ④ solvable but not supersolvable, ⑤ not solvable or simple, ⑥ simple; and for a group \( G \) in ③ , let \( B(G) \) represent \{groups \( H \) in ①+⑥ \mid \( k(H) \leq k(G) \}\} where \( j \) is the minimum positive integer.
such that $B(G)$ is non-empty. I conjecture that for any group $G$, if $B(G)$ exists then it contains some group $H$ such that $|H| > |G|$. As a check, note that the groups in section 2.3 are classified as follows: $(2.3.8)$ and $(2.3.18)$ are in (2); $(2.3.1)$, $(2.3.2)$, $(2.3.4)$, $(2.3.5)$, $(2.3.9)$, $(2.3.10)$, $(2.3.14)$, $(2.3.15)$, $(2.3.16)$, $(2.3.17)$, $(2.3.22)$, and $(2.3.23)$ are in (3); $(2.3.3)$, $(2.3.6)$, $(2.3.12)$, $(2.3.13)$, and $(2.3.21)$ are in (4); $(2.3.19)$ is in (5); and $(2.3.7)$, $(2.3.11)$, and $(2.3.20)$ are in (6). We have seen in section 2.1 and in $(2.2.7)$ that this conjecture is true for $G$ in (1).

Upon the slim evidence of $k = 5$, 6, and 7, the following seem true. For a given number $r$, let $k(G) = r$ and in $(1.1.4)$ suppose $m_k \neq r - 1$. Over the set of all such groups $G$, $|G|$ is a maximum if (i) $m_2$ is a minimum, (ii) the number of prime divisors of $|G|$ is a maximum, or (iii) the largest prime dividing $|G|$ is a minimum, $G$ not nilpotent.
Chapter Three

Groups of Prime Power Order

Section 3.1: The Duality Principle.

In Chapter 1 we used a method developed by Landau [22] and in Chapter 2, one of Burnside [8]. In this chapter, we introduce yet another approach to the problem of finding low upper bounds for the orders of groups with \( k \) classes.

(3.1.1) Theorem: Let \( S \) be a given set of groups, and let \( f_\mathbf{g} \) be a strictly monotonic increasing real function whose domain \( D_{f_\mathbf{g}} \) contains \( \{o(G) \mid G \in S\} \). If for every \( G \in S \), \( k(G) \geq f_\mathbf{g}(|G|) \), then for any \( k \) in \( f_\mathbf{g}(D_{f_\mathbf{g}}) \), \( f_\mathbf{g}^{-1}(k) \) is an upper bound for the order of any \( G \in S \) satisfying \( k(G) \leq k \).

Proof: Take \( k \) in the range of \( f_\mathbf{g}, f_\mathbf{g}(D_{f_\mathbf{g}}) \). Let \( G \in S \) have order \( g > f_\mathbf{g}^{-1}(k) \). Since \( f_\mathbf{g} \) is strictly monotonic increasing \( f_\mathbf{g}(g) > k \). Therefore \( k(G) > k \) by the conditions on \( f_\mathbf{g} \).

Q.E.D.

In particular, \( |G| \leq f_\mathbf{g}^{-1}(k(G)) \), directly from \( k(G) > f_\mathbf{g}(|G|) \) and \( f_\mathbf{g} \) monotonic increasing. 
The principle involved in (3.1.1) will be referred to as the Duality Principle. As an illustration of this process, we have the following simple theorem.

(3.1.2) Theorem: Let $S = \{\text{non-abelian 2-groups } G | G \text{ has a cyclic subgroup of index 2}\}$. Then $|G| \leq 4(k(G) - 3)$.

Proof: Let $G \in S$, $|G| = g = 2^m$. By (2.2.58), $k(G) = 2^{m-2} + 3$ or $2^{m-1} + 2^{m-2} - 2^{m-3}$. Now $2^{m-2} + 3 \leq 2^{m-2} + 3(2^{m-3}) = 2^{m-1} + 2^{m-2} - 2^{m-3}$ since $m \geq 3$ for $G \in S$. Hence if we let $f_s(g) = g/4 + 3$ then for $G \in S$, $f_s(g) \leq k(G)$. Obviously $f_s$ is strictly monotonic increasing. Therefore by (3.1.1), $g \leq f_s^{-1}(k(G)) = 4(k(G) - 3)$. 

Q.E.D.

In section 3.2 we propose to find an upper bound for the order of a p-group with a given class number by finding a lower bound for $k(G)$ if $G$ is a p-group and then turning this around by the Duality Principle. In section 3.3 we investigate whether, in particular, this result is a least upper bound for 2-groups. Unfortunately it is not and neither is the next possible value. We show that the problem of finding the group $G$ with maximum order (non-composite) for a given class number $k$ is complicated by changes in the structure of $G$ as $k$ increases. No conjectures are made although it seems that the groups with greatest ratio of order to class number will be 2-groups, for all orders.
Special Notation For This Chapter: We stated the notation \([x,y] = x^{-1}y^{-1}xy\) in section 1.2. The corresponding notation \([H,K] = \langle [x,y] | x \in H, y \in K \rangle\) is natural. We extend this with \([x,H] = \{[x,y] | y \in H\} = x^{-1}K_H(x)\) where \(K_H(x) = \{y^{-1}xy | y \in H\}\). The upper and lower central series of a p-group \(G\) play a very important role. By the upper central series is meant (M. Hall [14], 10.2) the series of characteristic subgroups \(Z_0 < Z_1 < Z_2 < \cdots < Z_{i+1} < \cdots < Z_c\) where \(Z_0 = 1, Z_c = G, Z_{i+1}\) is such that \(Z_{i+1}/Z_i = Z(G/Z_i)\), and \(Z_i \neq Z_{i+1}\) \((i=0,1,\ldots,c-1)\). \(G\) is said to have nilpotent class \(c\). Although this notation is standard, that of the lower central series is not. Hall [14] and Blackburn [2], the major sources for Chapter 3, use \(T_i\); because of the typescript, we are forced (by constant use) to change to the notation \(H_i\) employed by P. Hall [16] in a well-known fundamental paper on such series. Thus the lower central series of \(G\) will be the characteristic series \(H_2 > H_3 > \cdots > H_c > H_{c+1}\) where \(H_2 = [G,G], H_{c+1} = 1, H_{i+1} = [H_i,G],\) and \(H_i \neq H_{i+1}\) \((2 < i < c)\). Usually one lets \(H_1 = G\) so that the above rules can be extended to \(i = 1\), but Blackburn [2] has introduced the notion (which we adopt) of \(H_i\) defined by \(H_i/H_4 = C_{G/H_4}(H_2/H_4)\). Then \(H_i\) too is characteristic in \(G,\)
Blackburn has defined a CF $p$-group as one in which $|H_i/H_{i+1}| = p$ for $2 \leq i \leq c$, and an ECF $p$-group as a CF $p$-group with $G/H_2$ elementary abelian. For a CF $p$-group he has shown that $|G/H_1| = |H_1/Z_{c-1}| = p$.

(3.1.4) **Definition:** A CF $p$-group is said to have degree of commutativity $k$ (after Blackburn [2]) if $[H_i, H_j] \leq H_{i+j+k}$ for all $1 \leq i \leq j \leq c$. It is well-known (P. Hall [16]) that every $p$-group has degree of commutativity at least $0$.

Finally we reproduce a result of Hirsch [18], restricted to $p$-groups, because we will refer often to it.

(3.1.5) **Theorem:** If $G$ is a $p$-group of order $g$ and with class number $k$ then $g \equiv k \pmod{2(p^2-1)}$ if $p$ is odd, and $g \equiv k \pmod{3}$ if $p = 2$. 
Section 3.2: p-Groups With Minimum Class Number.

(3.2.1) Theorem: Let $p$ be a prime and let $G$ be a group of order $p^{2n+e}$, $n \in \mathbb{N}^+$, $e = 0$ or $1$, and denote $2n+e$ by $m$. Then $k(G) \geq n(p^2 - 1) + p^e = n(p^2 - 1) + e(p-1) + 1$.

Proof: We proceed by induction. For $m = 0$, $n(p^2-1)+p^e = 1 = |G| = k(G)$ with $G = 1$. Assume then that the theorem is proved for all $p$-groups of order $p^i$, $i < m$. Let $G$ have order $g = p^m$, $Z = Z(G)$ have order $p^m$, and $\overline{m} = 2m + e$ where $\overline{m} \in \mathbb{N}^+$, and $\overline{e} = 0$ or $1$. By (2.2.29), $k = k(G) \geq k(G/Z) + |Z| - 1$.

Now $|G/Z| = p^{m-\overline{m}}$ with $m - \overline{m} = 2(n - \overline{n}) + (e - \overline{e})$. If $(e - \overline{e}) = 0$ or $1$, then $k(G/Z) \geq (n - \overline{n})(p^2 - 1) + (e - \overline{e})(p-1) + 1$ by the induction assumption, for the order of the center of a $p$-group is greater than $1$. Substituting, we have $k \geq n(p^2 - 1) + e(p-1) + 1 + (p^m - [\overline{m}(p^2 - 1) + \overline{e}(p-1) + 1])$.

Since $Z$ is abelian, $p^\overline{m} = k(Z) \geq \overline{m}(p^2 - 1) + \overline{e}(p-1) + 1$ by the induction assumption, and hence $k \geq n(p^2 - 1) + e(p-1) + 1$.

For the case of $(e - \overline{e}) = -1$, then $m = 2n$, $\overline{m} = 2n+1$, and $m - \overline{m} = 2(n - (n+1)) + 1$. Therefore by the induction assumption and (2.2.29) again, $k \geq [n - (\overline{n}+1)](p^2 - 1) + p + (p^\overline{m}) - 1 = n(p^2 - 1) + 1 + [p^\overline{m} - (\overline{n}+1)p^2] + (p+\overline{m}-1)$.
Obviously $p + n - 1 > 0$. Now for $u \geq 4$ and $v \geq 0$, $u^{v} + 1 / 2 \geq 2 \cdot 4^{v} \geq v + 2$ since the graphs of $y = 2 \cdot 4^{v}$ ($v \geq 0$) and $y = v + 2$ ($v \geq 0$) intersect only at $v = 0$ while the former is concave up. Therefore, if $\Pi \geq 1$, $(p^{2})^{\Pi - 1 / 2} \geq \Pi + 1$ or $p^{2\Pi + 1} \geq (\Pi + 1)p^{2}$.

It remains only to show that for $m = 2n$, $m = 1$, and $m - m = 2(n-1) + 1$, $k \geq n(p^{2}-1) + 1$. Still we have $k \geq k(G/Z) + |Z| - 1 \geq (n-1)(p^{2}-1) + p + (p) - 1$. By (3.1.5) $g \equiv k \pmod{p^{2}-1}$. Here $g = p^{2n} \equiv 1 \pmod{p^{2}-1}$ while $k = (n-1)(p^{2}-1) + a + 1 \equiv a + 1 \pmod{p^{2}-1}$ for some $a > 0$ by the above calculations. Therefore $a \equiv 0 \pmod{p^{2}-1}$ or $a = b(p^{2}-1)$, $b \in J^{+}$. Thus, $k = (n-1)(p^{2}-1) + b(p^{2}-1) + 1 > n(p^{2}-1) + 1$, and we are done.

Q.E.D.

(3.2.2) Theorem: If $G = g = p^{2n+e}$ ($n \in J^{+}$, $e = 0$ or $1$) and $k(G) = k = n(p^{2}-1) + p^{e}$ satisfy (3.1.5).

Proof: If $p = 2$, then $g = 2^{2n+e} = (4)^{n}2^{e} \equiv 2^{e} \equiv n(3)+2^{e} = k$ modulo 3. If $p$ is odd we begin by using $p^{4} = (p^{2}+1)(p^{2}-1)+1 \equiv 1 \pmod{2(p^{2}-1)}$. If $g = p^{4j+e}$ ($j \in J_{0}^{+}$, $e = 0$ or $1$) then $g \equiv p^{e} \equiv 2j(p^{2}-1) + p^{e} = k \pmod{2(p^{2}-1)}$; if $g = p^{4j+2}$ ($j \in J_{0}^{+}$) then $g \equiv p^{2} \equiv (p^{2}-1)+1 \equiv (2j+1)(p^{2}-1)+1 = k \pmod{2(p^{2}-1)}$; if $g = p^{4j+3}$ ($j \in J_{0}^{+}$) then $g \equiv p^{3}$ and $k = (2j+1)(p^{2}-1) + p \equiv p^{2}+p-1$, modulo $2(p^{2}-1)$, and since $(p-1)(p^{2}-1) \equiv 0 \pmod{2(p^{2}-1)}$ then $p^{3}-p^{2}+p-1 \equiv 0$ or $p^{3} \equiv p^{2}+p-1 \pmod{2(p^{2}-1)}$. Q.E.D.
This indicates that it should be possible to construct a group $G$ of order $p^{2n+e}$ with class number $n(p^2-1) + p^e$.

Since this is the minimum class number, the classes should be as large as possible. Let $x \in G$ such that $|K(x)|$ is a maximum. Obviously $x \notin Z(G) = Z$, but $C(x) \supseteq \langle x, Z \rangle$ which then has order at least $p^2$, so $|K(x)| \leq p^{m-2}$ where $m = 2n+e$.

To have $|K(x)| = p^{m-2}$ we require $|Z| = p$ first. Then we continue by induction to show that $|Z_i/Z_{i-1}| = p$ and $|Z_i|=p^i$ for $i=1,2,...,m-2$. Suppose $|Z_i/Z_{i-1}| > p^2$ instead, so that $|K_G/Z_{i-1}(xZ_{i-1})| \leq p^{(m-i+1)-3}$, provided $|G/Z_{i-1}| > p^2$. By (2.2.27) then $|K_G(x)| \leq p^{(m-i+1)-3}p^{i-1} = p^{m-3}$, a contradiction. Of course when $i = m-2$, $|Z_i| = |Z_{m-2}| = p^{m-2}$ so $G/Z_{m-2}$ has order $p^2$ and is abelian. The induction process ends and $Z_{m-1} = G$ or $G$ has nilpotent class $c = m-1$. By construction $G$ is also an ECF $p$-group (see (3.1.3)). Since $H_i \leq Z_{m-i}$ for $i = 2,...,m$ (Hall [14], p.151), then by (3.1.3) $H_i = Z_{m-i}$. Thus we have the characteristic series $G > H_1 > H_2 = Z_{m-2} > H_3 = Z_{m-3} > ... > H_{m-1} = Z > 1$ where successive factor groups have order $p$.

By the definition of $H_1$ in (3.1.3) and the induction proof above, $x \notin H_1$. Let $y_1 \in H_1 - H_2$. Define $y_i = [x, y_{i-1}]$ for $i = 2,...,m-1$. By induction each $y_i \in H_i - H_{i+1}$; indeed,
$[x, y_{i-1}] \in [G, H_{i-1}] = H_i$ while $[x, y_{i-1}] \in H_{i+1} = Z_{m-i-1}$ implies that the image of $x$ in $G/Z_{m-i-1}$ commutes with the images of itself, $y_{i-1}$, and $y_i$ which generate a group of order at least 8 over $Z_{m-i-1}$, contradicting $|K(x)| = p^{m-2}$ as before by (2.2.27).

By (3.1.4), $[H_2, Z_2] = 1$. But $Z_2 = \langle y_{m-2}, y_{m-1} \rangle$ with $C_G(y_{m-1}) = G$. Since $[x, y_{m-2}] = y_{m-1}$, then $1 \neq K(y_{m-2})!$ and $K(y_{m-2}) = y_{m-2}[y_{m-2}, G] \leq y_{m-2}[H_{m-2}, G] = y_{m-2}Z$ of order $p$; it follows that $K(y_{m-2}) = y_{m-2}Z$ and $C_G(y_{m-2}) = C_G(Z_2)$ has order $p^{m-1}$. To facilitate this, we take $H_1 = C_G(Z_2) = C_G(y_{m-2})$ and continue, making $H_i = C_G(y_{m-i})$, restricting $m-i \geq i-1$ or $2 \leq i \leq (m+1)/2$. This means that $|K(y_{m-i})| = p^{i-1}!$ and because $K(y_{m-i}) = y_{m-i}[y_{m-i}, G] \leq y_{m-i}[H_{m-i}, G] = y_{m-i}H_{m-i+1}$ of order $p^{i-1}!$, $K(y_{m-i}) = y_{m-i}H_{m-i+1}$, its maximum. Since $[H_{i-1}, H_{m-i+1}] = 1$ and $H_{m-i} = \langle y_{m-i}, H_{m-i+1} \rangle$, then for $2 \leq 1 \leq (m+1)/2$ still, we have $H_{i-1} = C_G(Z_1)$ also. Conversely, if $H_{i-1} = C_G(Z_1)$, we can derive, by the same reasoning, that $H_{i-1} = C_G(y_{m-i})$. Lastly we note that if $i > (m+1)/2$ (and $i < m$) then $C_G(y_{m-i}) = \langle H_{i-1}, y_{m-i} \rangle$ since $[H_{m-i}, H_{i-1}] = 1$ but $[H_{m-i}, y_{i-1-j}] \neq 1$ for any $j > 0$, from the above. Let us now compute $k(G)$. 


If \( z \in G - H_1 \), then \( C_G(z) = \langle y_{m-1}, z \rangle \) since \( C_G(y_{m-1}) = \langle H_{i-1}, y_{m-1} \rangle \) for \( i > 1 \). Hence \( |K(z)| \leq p^{m-2} \) and \( G - H_1 \) splits into at least \( \frac{p^m - p^{m-1}}{p^{m-2}} = p^2 - p \) classes. Then if \( i > (m+1)/2 \), \( C_G(y_{m-1}) = \langle H_{i-1}, y_{m-1} \rangle \) so \( |K(y_{m-1})| \leq p^{i-2} \) and \( H_{m-1} - H_{m-1+1} \) splits into at least \( \frac{p^i - p^{i-1}}{p^{i-2}} = p^2 - p \) classes. On the other hand, if \( i \leq (m+1)/2 \) (and \( i \geq 2 \) of course), \( C_G(y_{m-1}) = H_{1-1} \) and \( |K(y_{m-1})| = p^{i-1} \) so \( H_{m-1} - H_{m-1+1} \) splits into \( \frac{p^i - p^{i-1}}{p^{i-1}} = p - 1 \) classes. Finally if \( i = 1 \), we are left only with \( Z \) which splits into \( p = (p-1) + 1 \) classes. Therefore \( k(G) \geq (p^2 - p)(m-1)/2 + (p-1)(m+1)/2 + 1 \) if \( m \) is odd, and \( k(G) \geq (p^2 - p)(m/2) + (p-1)(m/2) + 1 \) if \( m \) is even. When reduced, we have \( k(G) \geq n(p^2 - 1) + p^e \). To ensure equality we must have \( (y_{m-1})^p \in H_{i-1} \) for \( i > (m+1)/2 \).

(3.2.3) Theorem: Let \( G \) have order \( p^m \), \( m = 2n+e \), \( n \in \mathbb{N} \), 

\( e = 0 \) or \( 1 \), and assume (i) \( G \) has nilpotent class \( m-1 \), and (ii) \( C_G(y_{m-1}) = \langle H_{i-1}, y_{m-1} \rangle \) with \( (y_{m-1})^p \in H_{i-1} \) \( (1 < i < m) \) where \( G > H_1 > \cdots > H_m = 1 \) is the lower central series of \( G \) and \( y_{m-1} \in H_{m-1} - H_{m-1+1} \). Then \( k(G) = n(p^2 - 1) + p^e \).

The outline of the structure of \( G \) is given in Burnside [7], p.124; for more details see also Blackburn [2].
(3.2.4) **Theorem:** Let \( p \) be a given prime number and \( G \) any group of order a power of \( p \). Then \( |G| \) is bounded above by \( \frac{2(k(G)-1)}{p^2-1} \) or \( \frac{2(k(G)-p)}{p^2-1} + 1 \), depending upon which \( k(G) \) is integral.

**Proof:** The prime \( p \) is fixed. Let \( S = \{ \text{groups } G \mid \text{there exists some } m \in J_0^+ \text{ so } |G| = p^m \} \). Write \( g = |G| \) and \( m = 2n + e \) with \( n \in J_0^+ \) and \( e = 0 \) or \( 1 \). Over \( \{ g \mid g \in S \} \), define the function \( f_g \) by \( f_g(g) = n(p^2 - 1) + p^e \). By (3.2.1), if \( g \in S \) then \( k(g) \geq f_g(g) \). Also, \( f_g \) is strictly monotonic increasing. Indeed, if \( g = p^{2j} \) then \( f_g(g) = j(p^2 - 1) + 1 \); if \( g \) assumes the next largest value in the domain of \( f_g \) then \( g = p^{2j+1} \) and \( f_g(g) = j(p^2 - 1) + p \); and if \( g \) takes on the next value, \( p^{2j+2} \), then \( f_g(g) = (j+1)(p^2 - 1) + 1 = j(p^2 - 1) + p^2 \). Thus \( f_g \) satisfies the conditions of the Duality Principle.

Now by (3.1.5), \( k \equiv g = p^{2n+e} = p^e \pmod{p^2-1} \). Suppose \( k(G) \equiv 1 \pmod{p^2-1} \). Then \( g = p^{2n} \) (for some \( n \in J_0^+ \)) so that \( f_g(g) = n(p^2 - 1) + 1 \leq k(G) \). By (3.1.1), \( g \leq p^a \) where \( a = \frac{2(k(G)-1)}{(p^2-1)} \) which is integral by \( k(G) \equiv 1 \pmod{p^2-1} \).

On the other hand if \( k(G) \equiv p \pmod{p^2-1} \) so \( g = p^{2n+1} \pmod{p^2-1} \), then \( f_g(g) = n(p^2 - 1) + p \leq k(G) \) and by (3.1.1) \( g \leq p^a \) with \( a = \frac{2(k(G)-p)}{(p^2-1)} + 1 \) here, again integral since \( k(G) \equiv p \pmod{p^2-1} \).
Lastly, it is impossible that both values of the upper bound be integral for a given \( k(G) \), for then \( (p^2-1) \) divides \( 2(k(G)-1) \) and \( 2(k(G)-p) \) and hence \( 2(p-1) \), which implies
\[
(p^2-1) \leq 2(p-1) \text{ or } (p-1)^2 \leq 0.
\]
Q.E.D.

As a more general but less accurate result, we have:

(3.2.5) **Corollary:** Let \( p \) be a given prime number and let \( G \) be a group of order \( p^m \), \( m \) an arbitrary positive integer. Then \( m \leq 2(k(G)-p)/(p^2-1) + 1 \).

Now we may state the most general result on \( p \)-groups.

(3.2.6) **Theorem:** If \( G \) is a group with non-composite order, then \( k(G) \leq k \) only if \( |G| \leq 2(2k-1)/3 \).

**Proof:** By (3.2.1), if \( G \) is a group of order \( p^{2n+e} \), \( n \in \mathbb{N} \) and \( e = 0 \) or 1, then \( k(G) \geq n(p^2-1) + p^e \). If \( m = 2n+e \), then \( n(p^2-1) + p^e \) is \( \frac{m}{2}(p^2-1) + 1 \) or \( \frac{(m-1)}{2}(p^2-1) + p \). Now
\[
\left(\frac{m-1}{2}\right)(p^2-1) + p = \frac{m}{2}(p^2-1) + \frac{(1+2p-p^2)/2}{2} \text{ and } (1+2p-p^2)/2 < 1
\]
since \( 1+2p-p^2 = 2 - (p^2-2p+1) = 2 - (p-1)^2 < 2 \). Thus if \( G \) has order \( p^m \), \( k(G) \geq \left(\frac{m-1}{2}\right)(p^2-1) + p \).

For \( k = 1 \) or 2, and \( k(G) \leq k \), \( g = |G| = 1 \) or 2 and the theorem is true.
Let \( S = \{ \text{groups } G \text{ there exists a prime } p \text{ with an integer } m \geq 0 \text{ so } |G| = g = p^m > 2 \} \). Let the function \( f_g \) be defined by \( f_g(x) = (2^{p-1})(\log x - 1)/2 + 2 = \frac{3}{2}(\log x) + \frac{1}{2} \).

\[
= (3\log_2 x + 1)/2 \quad \text{for } x > 0; \quad f_g \text{ is obviously strictly monotonic increasing.}
\]

If \( G \in S \) is abelian of order \( x = p^m \), then \( k(G) = x \) and \( f_g(x) = (3\log_2 x + 1)/2 \). Now \( (3\log_2 x + 1)/2x \) is continuous for \( x > 0 \) and reaches its maximum value of 0.795 at \( x = e/2^{1/3} \).

Therefore for \( x \geq 3 \), \( (3\log_2 x + 1)/2x < 1 \) or \( f_g(x) < k(G) \).

Suppose now that \( G \in S \) is non-abelian of order \( x = p^m \), so \( m = \log_p x \geq 3 \). Now \( f_g(x) \leq k(G) \) if \( f_g(x) \leq (p^2-1)(\log p - 1)/2 + p \) or \( 3\log_2 x + 1 \leq (p^2-1)(\log p - 1) + 2p \). Naturally this is true for \( p = 2 \). Thus for \( p > 2 \), we need \( (p^2-1)\log x - 3\log_2 x \geq p^2 - 2p - 1 + 1 = p^2 - 2p \); that is,

\[
\log_2 x \cdot \frac{(p^2-1-3\log_2 p)}{p^2-2p} \geq 1. \quad \text{Since } \log_2 x \geq 3, \text{ we only need } 3(p^2-1-3\log_2 p) \geq p^2 - 2p, \text{ or } 9\log_2 p \leq 2p^2+2p-3, \text{ and since } \log_2 p < p \text{ this reduces to } 2p^2 - 7p - 3 \geq 0. \quad \text{The roots of this quadratic are } -0.386 \text{ and } +3.886 \text{ and so these inequalities are established for } p > 3. \text{ If } p = 3 \text{ then we already have } 9\log_2 3 \leq 12 + 6 - 3 = 21 \text{ since } \log_2 3 < \log_2 4 = 2 < 21/9.
\]

Therefore for every \( G \in S \), \( k(G) \geq f_g(g) \) and the conditions of (3.1.1) are satisfied. The theorem follows directly.

Q.E.D.
Section 3.3: The Least Upper Bound For $2$-Groups.

Is it possible that the last result of the previous section, (3.2.6), is a least upper bound? That is, given any number $d$, do there exist groups $G$ with $k(G) > d$ and $|G| = 2(2k(G)-1)/3$? Such groups, by (3.2.6), would have minimum class number $k(G)$, and their orders would have odd exponent, by (3.2.5) and the proof of (3.2.6). First, if $|G| = 2^1 = 2$, then we must have $(2k(G)-1)/3 = 1$ or $k(G) = 2$ and obviously $G = \langle x \mid x^2 = 1 \rangle$ has order 2 and class number 2. Second, if $|G| = 2^3 = 8$, then we need $(2k(G)-1)/3 = 3$ or $k(G) = 5$ and by (2.3.8) the quaternion and dihedral groups satisfy this. Next, for $|G| = 2^5 = 32$, we need $(2k(G)-1)/3 = 5$ or $k(G) = 8$, but no group of order 32 has class number less than 11 (see Hall and Senior [15]). Since no list of groups of order $128 = 2^7$ exists, we cannot easily check further, but we have an indication that the result of (3.2.6) is not a least upper bound.

Therefore we will try to show that no group $G$ exists with $|G| = 2^{2n+1} \geq 32$ and $k(G) = 3n + 2$. To do this, we prove more generally that no group $G$ exists with $|G| = 2^{2n+e} \geq 32$ ($e = 0$ or 1) and $k(G) = 3n+2^e$. That is, for $2$-groups, the result of (3.2.1) is not a greatest lower bound for $k(G)$, and consequently the result of (3.2.4) is not a least upper bound for $|G|$. At the same time it means that the result of (3.2.6) is not a least upper bound.
Note that the groups of order $1 = 2^0$, $2 = 2^1$, and $4 = 2^2$ are abelian and have class numbers $1 = 3(0)+2^0$, $2 = 3(0)+2^1$, and $4 = 3(1)+2^0$ respectively. Also, by (2.3.8) and (2.3.18), there are non-abelian groups of orders $8 = 2^3$ and $16 = 2^4$ with class numbers $5 = 3(1)+2^1$ and $7 = 3(2)+2^0$ — namely the quaternion, dihedral, and semi-dihedral groups. Thus for $|G| = 2^{2n+e} < 32$, $k(G) = 3n+2^6$ is possible.

Now the quaternion, dihedral, and semi-dihedral groups of order $2^m$ have maximum nilpotent class, $m-1$, and so by (3.2.3) should have minimum class number. But it is well-known (Blackburn [2], corollary to (3.9)) that a 2-group with maximum nilpotent class has a cyclic subgroup of index 2. By (3.1.2) then, such a group $G$ has order at most $4(k(G)-3)$, which is strictly less than $2^{(2k(G)-1)/3}$ and $2^{(2k(G)-2)/3}$ of (3.2.4) if $k(G) \geq 8$ or the exponent of the order of $G$ is at least 5. Thus no group of order $2^{2n+e} \geq 32$ and satisfying (3.2.3) can have $k(G) = 3n+2^6$.

Hall and Senior [15] have shown that for $|G| = 2^5 = 32$, the minimum value of $k(G)$ is 11 [c.f. $3n+2^6 = 8$] and that for $|G| = 2^6 = 64$, the minimum $k(G)$ is 13 [c.f. $3n+2^6 = 10$].

(3.3.1) Theorem: No group of order $2^{2n+e}$ ($n \in \mathbb{Z}^+$, $e = 0$ or 1, $2n+e \geq 5$) has class number $3n+2^6$. 
Proof: Let G be a group with minimum order contradicting the statement of the theorem. At least $2n+e \geq 7$ for $|G| = 2^{2n+e}$. Since G is a 2-group, its center $Z$ is non-trivial and so G contains a normal subgroup $N$ of order 2 in Z. Now $N$ splits into 2 conjugate sets over G so by (2.2.27), $k(G/N) \leq k(G) - 1 = 3n + 2^e - 1$. If $e = 0$, then $k(G/N) \leq 3n = [3(n-1) + 2] + 1$ so by (3.2.1) and (3.2.2), $k(G/N) = 3(n-1)+2$ and $G/N$ satisfies the statement of the theorem ($|G/N| > 32$), contradicting the choice of G. If $e = 1$, $k(G/N) \leq 3n + 1$ and by (3.2.1), $k(G/N) = 3n+1$, again a contradiction. Hence no such group G exists.

Q.E.D.

(3.3.2) Theorem: If $|G| = 2^{2n+e}$ ($n \in \mathbb{N}^+$, $e = 0$ or 1, $2n+e \geq 5$) then $k(G) \geq 3(n+1) + 2^e$.

Proof: Direct from (3.3.1), (3.2.1), and (3.2.2).

Q.E.D.

Our inquiry now turns to the value $3(n+1) + 2^e$ as a possible greatest lower bound for the class numbers of 2-groups, whose order is greater than 16. As mentioned before, Hall and Senior [15] have demonstrated groups of orders 32 and 64 and class numbers 11 and 13. Although the 2-groups with maximum nilpotent class and order 32 have class number 11, those of order 64 have class number 19,
and so we must search for groups of another structure. The groups of order 32 and 64 whose class number is given by \(3(n+1) + 2^6\) and which do not have maximum nilpotent class are characterized by (i) their lower central series satisfies 
\[|G/H_2| = 2^3 = 8\] and 
\[|H_1/H_{1+1}| = 2 (1 \geq 2),\] and (ii) no member of the upper central series has index \(2^3\). We will now try to construct all groups of order \(2^7 = 128\) with minimum class number; for such groups, \(k(G) \geq 14\) by (3.3.2).

(3.3.3) **Notation:** For a \(p\)-group \(G\), let \((a_0, a_1, a_2, \ldots, a_b)\) be used to indicate that \(G\) has \(a_1\) classes of order \(p^1\) and that no class of \(G\) has order greater than \(p^b\). The form \((a_0, a_1, \ldots, a_b)\) will be called the **\(p\)-class vector** of \(G\).

(3.3.4) **Theorem:** If \(N \triangleleft G, N \leq Z\), then 
\[k(G/N) \leq k(G) - |N| + 1.\]
If 
\[k(G/N) = k(G) - |N| + 1,\] then \(N = Z\); if also \(G\) is a \(p\)-group, and \(G/Z\) has \(p\)-class vector \((a_0, a_1, \ldots, a_b)\), then \(G\) has \(p\)-class vector \((|Z|, 0, \ldots, a_0 - 1, a_1, \ldots, a_b)\), where \(a_0 - 1\) is the number of classes of \(G\) of order \(|Z|\).

**Proof:** In the notation of (2.2.21), let \(G = N + A_2 + \cdots + A_k\), each \(A_i\) the union of classes of \(G\), and so 
\[G/N = 1 + A_2 + \cdots + A_k\] which is its class equation. Since \(N \leq Z\), then 
\[|N| + (k - 1) \leq k(G).\] In the case of equality, each \(A_i (1 \geq 2)\) is a class of \(G\). But by (2.2.22) \(|A_i| = f(1) \cdot |N|\) and so over \(G, |K_j| = 1\) implies \(K_j \leq N\), giving \(Z \leq N\).
Finally, if $G$ is a $p$-group, $k(G/Z) = k(G) - |Z| + 1$, and $G/Z$ has $p$-class vector $(a_0, a_1, \ldots, a_b)$, then $a_1$ is the number of $A_j$ of order $p^j$ and hence, for $j \geq 2$, $A_j$ has order $p^j |Z|$. Since every element of $Z$ has class of order 1 over $G$, and since $|Z| + (a_0 - 1)|Z| + a_1 p |Z| + \cdots + a_b p^b |Z| = |Z| \cdot (a_0 + a_1 p + \cdots + a_b p^b) = |Z| \cdot |G/Z| = |G|$, then no elements of $G$ have classes with orders between 1 and $|Z|$. Therefore $G$ has $p$-class vector $(|Z|, 0, \ldots, 0, a_0 - 1, a_1, \ldots, a_b)$.

Q.E.D.

(3.3.5) Theorem: Let $G$ be a group of order $128 = 2^7$. Then $k(G) = 14$ only if $G$ has lower and upper central series: $G > Z_4 > H_2 > H_3 = Z_3 > H_4 = Z_2 > H_5 = Z_1 > 1$.

Proof: Suppose $|Z| = 4$. Now $Z$ must contain a group $N$ of order 2, normal in $G$, and by (3.3.4) $k(G/N) \leq 14 - 2 + 1 = 13$. Since $|G/N| = 64$, then $k(G/N) \geq 13$ by (3.3.2) and so $k(G/N) = k(G) - |N| + 1$. By (3.3.4) then $N = Z$, a contradiction. Therefore $Z$ has order 2.

If we form $G/Z$, then $k(G/Z) \leq 14 - 2 + 1 = 13$ by (3.3.4), while $|G/Z| = 64$ means $k(G/Z) \geq 13$ by (3.3.2). Thus $k(G/Z) = k(G) - |Z| + 1 = 13$. The upper central series of $G$ now follows as stated in this theorem from the upper central series of $G/Z$, mentioned above and given in Hall and Senior [15]. As M.Hall ([14], p.151) has shown
H_i \leq Z_{i+1} \ (i \geq 2), \ we \ need \ prove \ only \ that \ |G/G'| = 8. \ By
(2.2.29), \ Z \leq G', \ so \ G/G' \cong (G/Z)/(G'/Z) \cong (G/Z)/(G/Z)',
which \ has \ order \ 8 \ by \ the \ structure \ of \ G/Z.

Q.E.D.

It \ now \ follows \ by \ (3.1.3) \ that \ G \ has \ the \ following
characteristic \ series, \ where \ successive \ factor \ groups \ have
order \ 2:

(3.3.6) \quad G > H_1 > Z_4 > H_2 > H_3 = Z_3 > H_4 = Z_2 > H_5 = Z_1 > 1.

(3.3.7) \textbf{Theorem}: \ If \ |G| = 128 \ and \ k(G) = 14, \ then \ k(G/Z) = 13
and \ G/Z \ has \ degree \ of \ commutativity \ > 0.

\textbf{Proof}: \ We \ proved \ k(G/Z) = 13 \ in \ (3.3.5). \ Now \ for \ all \ groups
of \ order \ 64 \ and \ class \ number \ 13, \ the \ derived \ group \ is \ abelian
(Hall \ and \ Senior [15]) \ and \ hence \ (Blackburn [2], \ corollary \ to
(2.10)) \ G/Z \ has \ degree \ of \ commutativity \ > 0.

Q.E.D.

(3.3.8) \textbf{Theorem}: \ If \ |G| = 128 \ and \ k(G) = 14, \ then \ G^2 \leq Z_4,
H_1^2 \leq H_3, \ Z_4^2 \leq H_4, \ H_2^2 \leq H_4, \ H_3^2 \leq H_5, \ and \ [H_i, H_i]
\leq H_{i+2} \ for \ i = 1, 2, \ and \ 3.

\textbf{Proof}: \ These \ are \ translations \ of \ relations \ that \ hold \ mod \ Z
because \ of \ the \ isomorphism \ between \ G/Z \ and \ (one \ of) \ the
groups \ of \ order \ 64, \ class \ number \ 13, \ listed \ in \ Hall \ and
Senior [15].

Q.E.D.
(3.3.9) **Theorem:** If $|G| = 128$ and $k(G) = 14$, then $G$ contains elements $s$ and $s_1$ such that $G = \langle s, H_1 \rangle$, $H_1 = \langle s_1, Z_4 \rangle$, $Z_4 = \langle s^2, H_2 \rangle$, $H_1 = \langle s_1, H_{1+1} \rangle$, and 

$[s_1, s_4] = [s_2, s_3]$, where $s_1 = [s_{1-1}, s]$ $(1 = 2, 3, 4)$.

**Proof:** By Lemma (2.9) of Blackburn [2], everything follows except $Z_4 = \langle s^2, H_2 \rangle$. Since $G^2 \leq Z_4$ by (3.3.8), then $s^2 \in Z_4$. Suppose $s^2 \notin H_2$; since $H_1 \leq H_3$ by (3.3.8), and $G/H_2$ is abelian, then $G^2 \leq H_2$ and $G/H_2 \cong G/G' \sim (G/Z)/(G/Z)'$ is elementary abelian, contradicting the structure of $G/Z$ outlined in Hall and Senior [15]. Therefore $s^2 \in Z_4 = H_2$.

We put $H_5 = Z_1 = \langle s_5 \rangle$.

(3.3.10) **Theorem:** If $|G| = 128$ and $k(G) = 14$, then $G$ has p-class vector $(2, 1, 1, 5, 5)$.

**Proof:** By (2.2.29) $k(G/Z) \leq k(G) - |Z| + 1$ and so by (3.3.7) this must be an equality. The p-class vector of $G$ can be derived from that of $G/Z$ now by (3.3.4). Since $Z$ has order 2 and $G/Z$ has p-class vector $(2, 1, 5, 5)$ (by Hall and Senior [15], p.32), $G$ has p-class vector $(2, 1, 1, 5, 5)$.

Q.E.D.
(3.3.11) Theorem: If $|G| = 128$ and $k(G) = 14$, then the 14 classes $K_i$ of $G$ must satisfy: $K_1 + K_2 = Z$ and both have order 1; $K_3 = s_4H_5$ and has order 2; $K_4 = s_3H_4$ and has order 4; $K_5 = s_2H_3$, $K_6 + K_7 = s^2H_2$, $K_8 + K_9 = s_1H_2$ or $s^2s_1H_2$, and all five have order 8; and $K_{10} = H_1 - (K_3 + K_9)$, $K_{11} + K_{12} + K_{13} + K_{14} = sH_1$, and all five have order 16.

Proof: We have assumed $|K_i| \leq |K_j|$ if $i < j$ (see (1.1.5)). Since $|Z_1| = 2$, then $K_1 = 1$, $K_2 = \{s_5\}$, and both have order 1. By (3.3.4), the conjugate classes of $G$, aside from $K_1$ and $K_2$, are of the form $K + K_5$ where $K$ is a conjugate class of $G/Z$, and the theorem would be proved just by referring to the structure of $G/Z$ outlined in Hall and Senior [15]. However, Hall and Senior do not explicitly give the form of the classes of the groups of order 64; they would have to be calculated. Instead, we present a more constructive proof.

For $i = 2, 3, \text{ and } 4$, $K(s_i) = s_i[s_i,G] \leq s_iH_{i+1}$ of order $2^{5-1}$, and because $G$ has $p$-class vector $(2,1,1,5,5)$, we must take $K(s_i) = s_iH_{i+1} = K_{7-i}$ ($i=2,3,4$). Next, $C_G(s^2)$ $\leq \langle s,s_4,s_5 \rangle$ (the latter two because $[Z_4,H_4] = 1$ (P.Hall [16])) which has order at least 16 since $s^2 \not\in H_2$. Therefore $|K(s^2)| \leq 8$ and by the form of the $p$-class vector of $G$, $|K(s^2)| = 8$ and $K_6 = K(s^2)$. For the same reason $K_7 = Z_4 - K_6$. 
The remaining elements of $G$ fall into the distinct cosets $sH_2$, $s^{-1}H_2$, $ss_1H_2$, $s^{-1}s_1H_2$, $s_1H_2$, and $s^2s_1H_2$. Since $K(x) = x[x,G] \leq xH_2 \ (x \in G)$, each of these cosets is the union of classes of $G$. Since $G$ has $p$-class vector $(2,1,1,5,5)$, 5 of the elements $s$, $s^{-1}$, $ss_1$, $s^{-1}s_1$, $s_1$ and $s^2s_1$ have classes of order $16 = |H_2|$, while the remaining element must have 8 conjugates and its coset over $H_2$ must be the union of two classes of order 8. By (2.2.1) $C_G(s) = C_G(s^{-1})$ so $|K(s)| = |K(s^{-1})|$ and both must be 16. Similarly, $(ss_1)^{-1} = s^{-1}s_1^{-1} = s_2s^{-1}s_1^{-1}$ by the definition of $s_2$ in (3.3.9), so $(ss_1)^{-1} \in s^{-1}s_1^{-1}H_2 = s^{-1}s_1(s_1^{-2}H_2) = s^{-1}s_1H_2$ since $H_1^2 \leq H_3$ by (3.3.8). Therefore if $|K(s^{-1}s_1)| = 8$, then $K((ss_1)^{-1})$ is $K(s^{-1}s_1)$ or $s^{-1}s_1H_2 - K(s^{-1}s_1)$, each of order 8, and so $|K(ss_1)| = 8$ by (2.2.1). Again then $|K(ss_1)| = |K(s^{-1}s_1)| = 16$, and we are done. 

Q.E.D.

(3.3.12) Theorem: If $|G| = 128$ and $k(G) = 14$, then $G$ has degree of commutativity greater than zero.

Proof: The necessary and sufficient condition that $G$ have degree of commutativity $> 0$ is that $H_2$ be abelian (Blackburn [2], (2.10)). Since $[H_2, H_4] \leq H_6 = 1$ by (3.1.4), this reduces to the condition that $[s_2, s_3] = 1$, or $[s_1, s_4] = 1$ by (3.3.9).
Since $s_4 \in \mathbb{Z}_2 - \mathbb{Z}_1$, $s_4$ must have exactly 2 conjugates by (3.3.11). Thus we want $H_1 = C_G(s_4)$. Suppose $s_4$ commutes with some element $x$ of $G - H_1 = sH_1$. Then $C_G(x) \geq \langle x, H_4 \rangle$ which must have order at least 16 since $x^2 \in (sH_1)^2 \leq s^2H_2$ so $x^2 \notin H_2$. This contradicts (3.3.11).

Q.E.D.

(3.3.13) Theorem: Let $|G| = 128$ and $k(G) = 14$. In addition to the defining commutators for $s_2$, $s_3$, and $s_4$, and the commutators equal to 1, the following relations hold in $G$: 

$$[s, s_4] = s_5, [s_1, s_2] = s_2^2[s, s_1^2],$$

$$[s_1, s_3] = [s, [s_2, s_1]], [s_1, s_2] = s_2^2s_3, [s_2, s_2] = s_3^2s_4, [s_3, s_2] = s_4^2s_5, s_5^2 = 1, s_4^2 = 1, s_3^2 = s_5,$$

$$s_2^2 \in s_4H_5, s_1^2 \in H_3, s_4 \in H_5.$$

Proof: Since $C_G(s_4) = H_1$ by (3.3.12), then $[s, s_4] = s_5$. In general, 

$$[s, s_2] = s_1^{-1}(s^{-2}s_1s^2) = s_1^{-1}(s^{-1}s_1s_1+1)$$

$$= s_1^{-1}s_1s_1+1s_1+1 = s_1+1s_1+2$$

because $[s_1, s] = s_1+1 (i=1,2,3).$

Also 

$$[s_1, s_2] = s_1^{-1}(s^{-1}s_1^{-1}ss_1)s_1s_2 = (s_2^{-1}s_1^{-1})s_1^{-1}ss_1s_2$$

$$= s_2[s, s_1^2]s_2.$$ Because $s_2$ and $[s, s_1^2]$ are in $H_2$ and $H_2$ is abelian by (3.3.12), then $[s_1, s_2] = [s, s_1^2]s_2^2$. Now 

$$[s_1, s_3] = s_1^{-1}(s^{-1}s_2^{-1}ss_2)s_1s_3 = (s_2^{-1}s_1^{-1})s_2^{-1}ss_2s_1s_3$$

$$= s_2s^{-1}([s_1, s_2]s_2^{-1}s_1^{-1})s_1s_2[s_2, s_1]s_3$$

$$= s_2s^{-1}(s_2^{-1}[s_1, s_2])(ss_2^{-1}s_2[s_2, s_1])s_3.$$
= s_2(s_3^{-1}s_2^{-1}s_1^{-1})(s_1,s_2)s[s_2,s_1]s_3 = s_3^{-1}[s,[s_2,s_1]]s_3
= [s,[s_2,s_1]], because H_2 is abelian. All other commutators are trivial (except those defining s_2, s_3, and s_4 of course) by the definition of degree of commutativity.

Since [s_1,s] = s_{i+1}, then [s_1^2,s] = s_1^{-2}s_1^{-1}s_1^{-2}s
= s_1^{-1}s_1^{-1}s_1^{-1}s_1^{-1} = s_{i+1}^{-1}[s_{i+1},s_1]s_{i+1}^{-1} = s_1^{-1}[s_{i+1},s_1] as H_2 is abelian. Using the fact that s_3^2 \in H_3^2 \leq Z_1 by (3.3.8), and [s_3,s_2] = 1, we get [s_3^2,s] = s_4^2 and [s_3^2,s] \in [Z,G] = 1; therefore s_4^2 = 1. Because C_G(s)
= \langle s,s_3 \rangle has order 8 by (3.3.11), then s_4^2 \in Z. From

[s_1,s_2] = s_2^2s_3 \quad \text{we have} \quad [s_1,s_4] = s_1^{-1}s_1^{-4}s_1s_4
= s_1^{-1}s_1^{-2}s_1^{-2}s_3^{-1}s_2^{-1}s_3^{-1} = s_1^{-1}(s_1s_2^{-1}s_3^{-1})(s_2^{-1}s_3^{-1}s_4^{-1}s_5^{-1}) = s_2^{-4}s_5^{-2}s_5
= s_3^2s_5 \quad \text{because s_2^2 \in H_2^2 \leq H_4 by (3.3.8), H_4^2 = 1 as shown above, and [s_2^2,H_4] = 1 by (3.3.12). But we have shown s_4^2 \in Z, so [s_1,s_4] = 1 and s_3^2 = s_5. We already have [s_2^2,s] = s_3^{-2}[s_3,s_2] = s_5 now, so s_2^2 \in s_4H_5. That s_1^2 \in H_1^2 \leq H_3 was known from (3.3.8).

Q.E.D.
Note that the value of $s_2^2$ depends precisely upon the choice of value of $s_1^2$. Indeed, $[s_1, s_2] = 1$ implies $C_G(s_2) = \langle s_1, H_2 \rangle$, and $[s_1, s_2] = s_4s_5$ implies $C_G(s_2) = \langle H_2, s_2^2s_1 \rangle$ since $[s_2, s_2] = s_4s_5$, both contradicting $C_G(s_2) = H_2$ by (3.3.11). Therefore we are free to choose 8 values for $s_1$ in $H_3$ and 2 values for $s_4$ in $H_5$, and the other values will follow by (3.3.13). It is straightforward to check that each combination gives a group of order 128 with class number 14. We remark on a few collective properties of these groups, but omit the routine calculations. The notation $T_{23} a_1$ is that of Hall and Senior [15].

(3.3.14) Theorem: There exist exactly 16 groups $G$ of order 128 and class number 14; half satisfy $G/Z \cong T_{23} a_1$ and the other half satisfy $G/Z \cong T_{23} a_2$. In all cases, $G/Z$ has exponent 4.

We will attempt to repeat this process. Most of the proofs will be identical with those of (3.3.5) to (3.3.13). By (3.3.2), a group of order $256 = 2^8$ has class number at least 16.
(3.3.15) Theorem: If $|G| = 256$ and $k(G) = 16$ then $G$ has
the characteristic series $G > H_1 > Z_5 > H_2$
$> H_3 = Z_4 > H_4 = Z_3 > H_5 = Z_2 > H_6 = Z_1 > 1$ where
successive factor groups have order 2.

Proof: If $|Z| \geq 8$, then, for any $x \in G$, $|C_G(x)| \geq 16$ and so
$|K(x)| \leq 16$. Therefore $256 = |G| \leq 8 + (16 - 8)(16)$ by
(1.1.2), a contradiction.

If $|Z| = 4$, then $k(G/Z) \leq 16 - 4 + 1 = 13$ by (2.2.29).
Since $|G/Z| = 64$, $k(G/Z) \geq 13$ by (3.3.2), and we can apply
(3.3.4). $G/Z$ has p-class vector $(2,1,5,5)$ (Hall and Senior
[15], p.32), so $G$ has p-class vector $(4,0,1,1,5,5)$. Also by
(2.2.29), $G' \geq Z$. Hence $G/G' \sim (G/Z)/(G/Z)'$ which has order
8 by Hall and Senior, so $|G'| = 32$. If $G'$ were abelian, at
least 32 elements of $G$ would have centralizer of order $\geq 32$;
that is, at least 32 elements of $G$ would lie in classes of
order at most 8. This is a contradiction because the p-
class vector of $G$ is $(4,0,1,1,5,5)$, which means $G$ has
precisely 4 classes of order 1, none of order 2, 1 of order
4, and 1 of order 8. We must take $G'$ non-abelian.

Suppose $Z$ is cyclic, $Z = \langle z | z^4 = 1 \rangle$. If no element of
$G - Z$ has order 2, then $G$ has only one element of order 2 and
so has a cyclic subgroup of index 2 (Burnside [7], p.132).
By (2.2.58) such a group of order 256 would have class number at least 67. Therefore, let $x \in G - Z$ with order 2.

By (2.2.29) $xz \in K(x)$. But $|xz| = 4$ while $|x| = 2$, a contradiction. It follows that $Z$ must be elementary abelian.

Let $N \trianglelefteq Z$, $|N| = 2$, $N \lhd G$. Then $|G/N| = 128$ and $k(G/N) < 16$ by (2.2.28), so $k(G/N) = 14$ by (3.3.2) and (3.1.5). Now $G'/N \approx (G/N)'$ which is abelian by (3.3.12), so $G'' \leq N$.

Since $Z$ is elementary abelian, $N$ is not unique, so $G'' = 1$ or $G'$ is abelian. This is a contradiction; we must have $|Z| = 2$.

By (2.2.29), $k(G/Z) \leq 16 - 2 + 1 = 15$, so by (3.3.2) and (3.1.5) again, $k(G/Z) = 14$ and $G/Z$ has the structure of $G/Z$ and (3.3.6) and (3.3.13). This gives the upper central series of $G$. Since $|Z| = 2$, $Z \leq G'$ (Hall and Senior [15], p.8) and $G/G' \approx (G/Z)/(G/Z)'$ has order 8. The lower central series follows by (10.2.2) of M.Hall [14]. The placement of $H_1$ was determined in (3.1.3).

Q.E.D.

(3.3.16) Theorem: If $|G| = 256$, $k(G) = 16$, and $Z = \langle z \rangle$, then $k(G/Z) = 14$ and the classes of $G$ of order $\neq 1$ have the form $\overline{K} + \overline{K}z$ where $\overline{K}$ is a class of $G/Z$, except in one case where $\overline{K}$ and $\overline{K}z$ will yield distinct classes of $G$ of order $|\overline{K}|$. 
Proof: The first we proved in (3.3.15) and the second follows from (2.2.27).

Q.E.D.

(3.3.17) Theorem: If \(|G| = 256\) and \(k(G) = 16\), then \(G\) has degree of commutativity greater than zero.

Proof: Directly from (3.3.12) and (2.10) of Blackburn [2].

Q.E.D.

Note that the results of (3.3.8) still hold for \(G\) if \(|G| = 256\) and \(k(G) = 16\).

(3.3.18) Theorem: If \(|G| = 256\) and \(k(G) = 16\), then \(G\) contains elements \(s\) and \(s_1\) such that \(G = \langle s, H_1 \rangle\), \(H_1 = \langle s_1, Z_5 \rangle\), \(Z_5 = \langle s^2, H_2 \rangle\), and \(H_1 = \langle s_1, H_{1+1} \rangle\) where \(s_1 = [s_{i-1}, s] (i = 2, 3, 4, 5, 6)\).

Proof: By Lemma (2.9) of Blackburn [2], everything follows except \(Z_5 = \langle s^2, H_2 \rangle\), whose proof is obviously the same as in (3.3.9), and \([s_5, s] \in Z - 1\). For this latter, note that \([H_1, Z_2] = 1\) by (3.3.17) so \(C_G(s_5) \geq H_1\). Since \(s_5 \notin Z\), then \(C_G(s_5) = H_1\). But \([s, s_5] \in [G, H_5] = H_6 = Z\).

Q.E.D.

(3.3.19) Theorem: If \(|G| = 256\) and \(k(G) = 16\), then the following relations hold: \(s_6^2 = 1, s_5^2 = 1, s_4^2 = s_6, s_3^2 \in s_5 H_6\), and \(s_2^2 \in s_4 H_5\).
Proof: Obviously $s_5^2 = 1$. By (3.3.8) $[H_5^2, G] \leq [H_6, G] = 1$; we showed $[s_1^2, s] = s_1 [s_1 + 1, s_1]s_1 + 1$ in (3.3.13), so

$[s_4^2, s] = s_5[s_4, s_5]s_5 = s_5^2$ by (3.3.17) and hence $s_5^2 = 1$.

As shown in (3.3.13), $[s_1, s^2] = s_1 + 1^2 s_1 + 2$, so $[s_2, s^2]$

$= s_3^2 s_4 \in s_4 H_5$ by (3.3.8); therefore $[s_2, s^4] = s_2^{-1} s^{-4} s_2 s^4$

$= s_2^{-1} s^{-2}(s_2 s_3^2 s_4^2) s^2 = s_2^{-1}(s_2 s_3^2 s_4)(s_3^2)(s_4 s_2^2 s_4)$

$= s_3^4 s_4^2[s^2, s_4]$, using $[H_1, H_5] = 1$ by (3.3.17). But

$s_3^4 \in H_5^2 = 1$, $[s_2, s_4] = s_5^2 s_6 = s_6$, and $[s_2, s^4] \in [H_2, Z_5^2]$

$\leq [H_2, H_4] = 1$ by (3.3.17); therefore $s_4^2 = s_6$. Next

$[s_3^2, s] = s_3^2 s_3^2 = s_3^{-1}(s_4 s_2^2 s_4)(s_3^2) = s_4^2 [s_3, s_4] = s_6$

and hence $s_3^2 \in s_5 H_6$ by (3.3.13). In turn, $[s_2^2, s]$

$= s_3^2 [s_2, s_3] \in s_5 H_6$ by (3.3.17) and (3.3.8), so $s_2^2 \in s_4 H_5$.

Q.E.D.

(3.3.20) Theorem: There is no group of order 256 and
having class number 16.

Proof: By (3.3.8) $s_1^2 \in H_3$. Suppose $s_1^2 \in s_2 H_4$. From

(3.3.13), $[s_1, s_2] = s_2 [s, s_1^2]s_2 = s_2^2 [s, s_1^2]$ because

$[H_2, H_4] = 1$ by (3.3.17). It follows that $[s_1^2, s_2]$

$= s_1^{-2} s_2^{-1} s_1^2 s_2 = s_1^{-1}(s_2^2 [s, s_1^2] s_2^{-1})s_1 s_2$

$= (s_2^2 [s_2, s_1]) ([s, s_1^2] [[s, s_1^2], s_1]) (s_2^2 [s, s_1^2])$
= s_2^4[s,s_1^2][s_2^2,s_1][s_3^2,s_1] = (s_6)(s_6)[s_4,s_1][s_4,s_1]
using (3.3.19), \( s_1^2 \in s_3H_4 \), and (3.3.17). That is, \([s_1^2,s_2]\) = 1, and since \( s_1^2 \in s_3H_4 \) while \([H_4,H_2]\) = 1 by (3.3.17), then \( 1 = [s_1^2,s_2] = [s_3,s_2] \). Therefore \( C_G(s_2)^+ H_2 \) so \( K(s_2) \) has order at most 8. Under (3.3.4) and (3.3.10), \( G \) would have p-class vector \((2,1,1,5,5)\) and \( |K(s_2)| = 16 \) if \( k(G) = 15 \). Of course \( k(G) = 16 \) here, and one exception is allowed, by (3.3.16). This exception must be \( K(s_2) \), so \( G \) has p-class vector \((2,1,1,3,4,5)\). In particular, \( K(s_1) \) must have order greater than 8; only the elements of \( H_2 \) have centralizers of order at least 32. Now \([s_1,s_3]\) = \([s_1,s_4]\) since \( s_1^2 \in s_3H_4 \) so \( s_3 \in s_1^2H_4 \). But \([s_1,s_4]\) = \( s_1^{-1}(s^{-1}s_3^{-1}s_3)s_4 = (s_2s^{-1}s_1^{-1})s_3^{-1}a_3s_1s_4 \)
= \( s_2s^{-1}([s_1,s_3]s_3^{-1}a_3^{-1})s(s_1s_3[s_3,s_1])s_4 \)
= \( s_2s^{-1}[s_1,s_3]s_3^{-1}(s_2s^{-1})s_3[s_3,s_1]s_4 \)
= \( s_2s^{-1}[s_1,s_3](ss_4^{-1})(s_2^{-1}[s_2,s_3])[s_3,s_1]s_4 \)
= \( s_2s^{-1}[s_1,s_3]s_3^{-1}s_2^{-1}[s_2,s_3]s_4 \)
= \( s_2[s,[s_3,s_1]]s_4^{-1}s_2^{-1}[s_2,s_3]s_4 \) = \([s,[s_3,s_1]]s_2,s_3] \) using (3.3.17) and (3.3.18) only. Here \([s_2,s_3] = 1 \) and \([s_3,s_1] = [s_4,s_1] \in Z \) by (3.3.17), so \([s_1,s_4] = 1 \in [s_1,s_3] \). This means \( C_G(s_1) \geq <s_1,H_3> \) which has order at least 32, contradicting our statement above. Therefore \( s_1^2 \in H_4 \).
We had earlier \([s_1^2, s_2] = s_2^4[s, s_1^2]^2[s_2^2, s_1][s, s_1^2], s_1\)
so \([s_1^2, s_2] = (s_6)(1)[s_4, s_1](1) = s_6[s_4, s_1].\) But \([s_1^2, s_2]\)
\(\in [H_4, H_2] = 1\) so we derive \([s_4, s_1] = s_6.\) Now if \(s_1^2 \in s_4H_5\)
then \([s_4, s_1] \in [s_1^2H_5, s_1] = 1\) by (3.3.17), a contradiction.
Therefore \(s_1^2 \in H_5.\) Still \([s_1, s_4] = s_6,\) and as before
\([s_1, s_4] = [s_2, s_3][s, [s_3, s_1]].\) Now \([s_1, s_3] = s_1^{-1}s_3^{-1}s_1s_3 = \)
\(s_1^{-1}(s^{-1}s_2^{-1}s_2s_1)s_3 = (s_2s^{-1}s_1^{-1})s_2^{-1}ss_1s_3\)
\(= s_2s^{-1}([s_1, s_2]s_2^{-1}s_1^{-1})a(s_1s_2[s_2, s_1])s_3\)
\(= s_2s^{-1}[s_1, s_2]s_2^{-1}(s_2s^{-1})s_2[s_2, s_1]s_3\)
\(= s_2s^{-1}[s_1, s_2]s_2^{-1}s[2, s_1]s_3 = s_2s^{-1}s_2^{-1}[s_1, s_2]s_2[s_2, s_1]s_3\)
\(= s_2(s_3^{-1}s_2^{-1}s_1^{-1})[s_1, s_2]s_2[s_2, s_1]s_3 = s_2s_3^{-1}s_2^{-1}[s, [s_2, s_1]]s_3\)
\(= [s_3, s_2][s, [s_2, s_1]]\) using (3.3.17) and (3.3.18). If we
substitute \([s_2, s_1] = s_2^{-2}[s_1^2, s] derived in (3.3.13), use
\(s_2^6 = 1\) by (3.3.19), and substitute for \([s_3, s_1]\) in \([s_1, s_4]\)
we have \([s_1, s_4] = [s_2, s_3][s, [s_2^2s_3^{-2}, s], s][s_2, s_3]].\)
Now \([s_2, s_3] \in H_6\) by (3.3.17), while \([s, s_1^2] \in H_6\) by \(s_1^2 \in H_5,\)
\(s_2^2 \in s_4H_5,\) and \(s_2^4 \in H_6\) by (3.3.19). Upon substitution,
\([s_1, s_4] = [s_2, s_3](s_6).\) But originally \([s_1, s_4] = s_6.\) Hence
\([s_2, s_3] = 1\) and again we must have \((2, 1, 1, 3, 4, 5)\) as the
p-class vector of \(G.\) In particular, \(C_G(s_3) = C_G(s_2) = H_2.\)
To arrive at a contradiction, consider \([s_1, s_3]\) = \([s_2, s_3][s, [s_2, s_1]]\) (shown above). We have proved that 
\([s_1^2, s] = s_1 + 1^2[s_1 + 1, s_1]\) so \([s_1, s_3] = [s_2, s_3][s, s_2^{-2}[s_1^2, s]]\) = \([s_2, s_3][s, s_2^{-2}]\) since \([s_1^2, s] \in [H_5, s] = H_6\). But \(s_2^8 = 1\) so \(s_2^{-2} = s_2^6 \in s_2^2H_6\) by (3.3.19). Hence \([s_1, s_3]\) = \([s_2, s_3][s, s_2^2]\) = \(s_3^{-2} = s_3^2\) by the relation on \([s_1^2, s]\) above. Now \(s^4 \in H_6\) since the p-class vector gives \(C_G(s) \geq \langle s, s_6 \rangle\) as having order 8. Thus \(1 = [s_1, s_4]\) = \(s_4^4s_3^2[s_2^2, s^2][s_3, s^2]\) as derived in (3.3.13). Since 
\([s_2^2, s] = s_3^2[s_3, s_2] = s_3^2\), then \([s_2^2, s^2] = s_3^4s_4^2\). In (3.3.13) we demonstrated that \([s_3, s^3]\) = \(s_4^2s_5\). Upon substitution \(1 = (s_6)(s_3^2)[(s_3^{4s_4^2})(s_4^2s_5)] = s_5s_6s_3^2\).

Therefore \(s_3^2 = s_5s_6\). Thus our evaluation of \([s_1, s_3]\) gives 
\([s_1, s_3] = s_5s_6\). But \([s_3, s^2] = s_4^2s_5 = s_6s_5\) by (3.3.19). Therefore \(s^2s_1 \in C_G(s_3)\), which conflicts with the p-class vector of \(G\). This means no value of \(s_1^2 \in H_3\) gives group relations free of contradiction.

Q.E.D.

By exactly the same proof as in (3.3.2), we conclude:

(3.3.21) Theorem: If \(|G| = 2^{2n+e}\) \((n \in J^+, e = 0 \text{ or } 1, 2n+e \geq 8)\) then \(k(G) \geq 3(n+2) + 2^e\).
CHAPTER FOUR

OTHER AUTHORS

In this short and final chapter, I would like to mention the work of some authors which was not used in the derivation of the results in the previous chapters, but which is related closely to certain aspects of these results. I hope that these articles will stimulate more research on the group class equation, and in particular on the problem of characterizing the groups of maximum order with a given number of classes. At least they will indicate the range of studies made on topics in this field.

One of the most common situations in the group class equation (1.1.4), because of (2.2.17) and the low values of $k$ taken, was that in which all $m_i$ were prime powers. In fact, this was the case for the groups of highest order and class numbers 5, 6, and 7, and hence is worthy of closer study. Having all $m_i$ non-composite implies every element of the group must have prime power order. G.Higman [17] has studied such groups and shown that the solvable ones have a much simpler structure than the
non-solvable. One generalization of this situation has been studied just recently by O.Grun [13]; he obtained rather general results on groups whose elements have order either a power of a given prime p or have order relatively prime to p.

A second type of generalization, from the case of having all $m_i$ prime powers, is to take groups in which the centralizer of any element is nilpotent — so-called CN-groups. These were intensively studied during the period 1955 - 1960 with very good results. For a summary and bibliography on this, we refer to M.Suzuki [35]; as he states, "the purpose of this paper is to clarify the structure of finite CN-groups."

The particular case of having some $m_1$ prime was studied in depth initially by R.Erauer [3] in 1943 and many authors followed in his footsteps. The case of $m_1 = 2$ had long been completed, and then, in the 1950's, using the theory of characters, a break-through was made on the case of $m_1 = 4$ by M.Suzuki([33] and [34]). With more recent work, Gorenstein and Walter [12] have given a detailed form of this result. As mentioned earlier, the case of $m_1 = 3$ has been solved recently too by Feit and Thompson [11].
Less research has been done on the order of the classes than on the indices. We have referred to an article by N. Ito [20] which studies groups having all non-trivial classes of the same order, and includes a generalization of a theorem of Tchounikhin (Cunihin) [36], one of the few early works in this area. At the same time R. Baer [1] published results on the case of some class having prime power order. Work in general on the topics of Chapter 2 has been done so repetitively by G.A. Miller that we refer to his collected works [26] only.

Few articles deal with p-groups from the point of view of either the orders or indices of their classes. H.G. Knoche [21] has derived bounds on the nilpotent class in the case that the orders of the conjugate classes of a p-group are at most p, p^2, and p^3. As mentioned in section 1.1, G.A. Miller [25] has shown (by substituting directly into a theorem similar to (2.2.29)) that the class number of a non-abelian p-group is at least p^2+p-1.

We note that the case of metacyclic groups can be studied by the methods of Chapter 3, using a result of Curtis and Reiner ([9], p.338).
SUMMARY

In 1903, E. Landau [22] proved that the order of a finite group with \( k \) conjugate classes must be bounded by some number \( f(k) \). We began by reproducing Landau's proof and then extended his method to derive the bound \( f(k) \) explicitly. The proof was based on the group class equation — a group is the union (sum) of its conjugate classes — in the form: the sum of the reciprocals of the indices of the classes of a group is unity; it used very little group theory. The logical question was then what restrictions can be placed on the latter equation (also called the group class equation in this thesis) using the theory of groups.

We proceeded to derive some of these conditions. As an application, we found those groups which have exactly 6 or 7 classes. (The groups with less than 6 classes had been discovered by Miller [23] and Burnside [8] about 1910; and while Sigley [32] claimed in 1935 to have found those with 6 classes, he presented almost no proof, and omitted one group.)
These results indicated the bound $f(k)$ on the order of a group with $k$ classes was much too high. We took the case of groups of prime power order and established, by methods almost as straightforward as those of Landau, although unrelated, a much truer bound. For groups of order a power of 2, this formula was only a least upper bound for small $k$; we made preliminary investigations that indicated the complications involved in finding such a least upper bound.
BIBLIOGRAPHY


[8] "Note A: on the equation $N = h_1 + h_2 + \cdots + h_r$", Theory of Groups of Finite Order, Dover, New York, 2nd ed. (1911).


[27] Neumann, B.H. "Groups with automorphisms that leave only the neutral element fixed", Arch.Math. 7 (1956), 1-5.


[34] --- "On finite groups containing an element of order four which commutes only with its powers", Ill.J. Math. 3 (1959), 255-271.


Letters:
