PRIME-POWER GROUPS

by

GERALD CLARK SCHRAG

A. B., Bethel College, 1960

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1964

Approved by:

Richard Yates
Major Professor

TABLE OF CONTENTS

INTRODUCTION

The theory of prime-power groups is very important in the application of finite group theory. This becomes apparent upon observation of Sylow's Theorem which is Theorem b listed later in this introduction. In fact it happens that any finite group may be generated by any set of these Sylow subgroups which contains one Sylow subgroup of each possible order.

The purpose of this report is to present in a logical order some of the basic properties of prime-power groups. To do this a basic knowledge of elementary finite group theory will be assumed on the part of the reader. Those theorems which are particularly important to this development are listed in the latter part of this introduction. Reference will be made to many of these throughout the paper. In addition a basic knowledge of permutations will be assumed.

Since this paper is not concerned in any way with groups that are not finite, henceforth the word "groups" will be used to mean finite groups.

The identity element of any group throughout the paper will be denoted by the letter "e". The group which is generated by the elements a, b, and c, for example, will be denoted by $\{a, b, c\}$. The permutation in which the element abc, for example, is replaced by the element dfg will be denoted as $\begin{pmatrix} abc \\ dfg \end{pmatrix}$.

The following is a list of definitions, theorems and corollaries which will be used throughout the paper.

DEFINITION a: If a and b are elements of a group G such that $b^{-1}ab = a$ for all b in G, then a is a self-conjugate element of G.

DEFINITION b: If H is a subgroup of a group G such that $b^{-1}Hb = H$ for all b in G, then H is a normal subgroup of G.

DEFINITION c: The set of all self-conjugate elements in a group G is the center of G.

DEFINITION d: A group G is an Abelian group if ab = ba for all elements a and b of G.

DEFINITION e: Let G be a group of order n and let H be a subgroup of G of order h. The quotient n/h is the index of H in G.

DEFINITION f: Let H be a normal subgroup of a group G. Consider all sets of the form aH where a is any element of G. These sets form a group which is called a factor group of G and is denoted by the symbol G/H.

DEFINITION g: A mapping $G \rightarrow H$ of the elements of a group G onto those of a group H is called a homomorphism if whenever $a_1 \rightarrow b_1$ and $a_2 \rightarrow b_2$, then $a_1 a_2 \rightarrow b_1 b_2$ where a_i is an element of G and b_i is an element of H for i = 1, 2.

DEFINITION h: If G is an Abelian group of order p^m where p is a prime number and m is a positive integer and G is the direct product of groups of order $p^{m_1}, p^{m_2}, \ldots, p^{m_n}$, then G is of type $(m_1, m_2, \ldots, m_n)$.

DEFINITION i: The set of all elements of the form $a^{-1}b^{-1}ab$, where a and b are any two elements of a group G, generate a subgroup of G which is called the commutator subgroup of G.

DEFINITION j: The elements of a group G which are permutable with a given subgroup H of G form a subgroup K of G which is called the normalizer of H in G.

THEOREM a: (Theorem of Lagrange). The order of a subgroup of a group G is a factor of the order of G.

COROLLARY 1: The order of an element of G is a factor of the order of G.

COROLLARY 2: Any cyclic group and hence any group whose order is a prime is an Abelian group.

THEOREM b: (Sylow's First Theorem). Let G be a group of order n and let p^r be the highest power of a prime p contained in n as a factor where r is a positive integer. Then G contains at least one subgroup of order p^r.

THEOREM c: (Cauchy's Theorem). If the order of a group G is divisible by a prime number p, then G has elements of order p.

THEOREM d: The center of a group G is a subgroup of G.

THEOREM e: A non-cyclic Abelian group G whose order is p^m, where p is a prime and m is a positive integer, is the direct product of cyclic groups no two of which have any element in common except the identity element.

THEOREM f: The elements common to the subgroups of a complete set of conjugate subgroups of a finite group G form a normal subgroup H of G.

THEOREM g: If Δ is the commutator subgroup of a given group G and H is any normal subgroup of G, then $\{H, \Delta\}/H$ is isomorphic to the commutator subgroup of G/H.

COROLLARY 1: If the normal subgroup H of G contains the commutator subgroup Δ of G, then G/H is Abelian.

COROLLARY 2: If G/H is Abelian, then H contains Δ.

THEOREM h: The elements of a group G which are permutable with a given subgroup H of G form a subgroup K of G which is either the same as H or contains H as a normal subgroup. The number of subgroups conjugate to H in G is equal to the index of K in G.

THEOREM i: The elements of a finite group G which are permutable with a given element b of G form a subgroup H of G. The number of elements conjugate to b in G is equal to the index of H in G.

THEOREM j: (Fermat's Theorem). If p is a prime, then $x^p \equiv x \bmod p$ for any positive integer x.

THEOREM k: The only subgroups of order 4 are the cyclic group $a^4 = e$ and the group defined by $a^2 = b^2 = e$, $ab = ba$.

GENERAL PROPERTIES OF PRIME-POWER GROUPS

In much of the literature on finite group theory reference is made to either prime-power groups or to p-groups.

DEFINITION 1: A group is a prime-power group if its order is a positive integral power of a prime number.

DEFINITION 2: A group is a p-group if every element of the group has order a non-negative integral power of a fixed prime number.

Many books which refer to one or the other of these two types of groups do not refer to both. This, along with the similarity of definitions, would lead one to believe that they are either very closely related or equivalent. The following theorem shows that they are equivalent.

THEOREM 1: A group G is a p-group if and only if it is a prime-power group.

Proof: If G is a prime-power group it is of order p^m where m is a positive integer and p is a prime number. Then by Corollary 1 of Theorem a, the order of every element of G is a divisor of p^m, that is a power of p. Hence G is a p-group.

For the second part of the proof assume that G is not a prime-power group. This means the order of G contains another prime factor q, where $q \neq p$. This implies, by Theorem c, that G has elements of order q and hence G is not a p-group.

LEMMA 1: A non-empty subset H of a group G is a subgroup of G if and only if it is closed with respect to the group operation.

Proof: (Recall that only finite groups are being considered and note that this theorem would not be true in general for groups of infinite order.) If H is a subgroup of G it is closed by one of the group postulates.

Conversely, let H be closed. Associativity of H follows directly from the associativity of G. Since G is of finite order every element of G is of finite order. Let a be an arbitrary element of H of order s. Then $a^s = e$ where e is the identity element of G. Since H is closed, $a^s = e$ is an element of H, and H contains the identity element of G. If $s = 1$, then $ee = e$ and the inverse e of e is in H. If $s \neq 1$, $aa^{s-1} = a^{s-1}a = a^s = e$. Thus the inverse of a is a^{s-1}. Since this is a power of a and H is closed it is in H. Thus every element of H has an inverse element in H since a was an arbitrary element of H. Therefore H is a subgroup of G.

Several theorems and corollaries will now be proven concerning self-conjugate elements and normal subgroups of prime-power groups. The first of these is the following important theorem.

THEOREM 2: A prime-power group G of order p^m contains a self-conjugate element of order p.

Proof: If G is Abelian every element a of G commutes with every other element of G. This implies that $a \neq e$ is self-conjugate in G. The order of a is a power of p. If G is non-Abelian let g be a non-self-conjugate element of G, and consider the complete set of conjugates to which g belongs. The elements which commute with g form a subgroup H of G. The number of elements conjugate to g in G is equal to the index of H in G. Since the order of H must be p^s where $s < m$, the number of elements conjugate to g in G is p^{m-s} or is a factor of p^m. Also since no two distinct complete sets of conjugates

have an element in common, the non-self-conjugate elements form disjoint sets, each of whose number of elements is divisible by p. Therefore the number of non-self-conjugate elements of G is a multiple of p, say kp. The number of elements of G other than the identity is $p^m - 1$. Let r be the number of self-conjugate elements of G other than the identity. Then $r + kp = p^m - 1$ or $r + 1 = p(p^{m-1} - k)$. This implies r + 1 is divisible by p. Thus r cannot be zero. Therefore there is a self-conjugate element a of G other than the identity. Its order must be a power of p. This has now been shown for G either Abelian or non-Abelian.

Now let the order of the self-conjugate element a in G be p^i where $0 < i \leq m$. This implies that $a^{p^i} = e$ and this is the least positive power of a such that this is true. Also $a^{p^i} = (a^{p^{i-1}})^p = e$. Since p is a prime, $a^{p^{i-1}}$ is either e or of order p. If it is e this contradicts the assumption that a is of order p^i since $p^{i-1} < p^i$. Therefore $a^{p^{i-1}}$ is an element of order p. Since a is self-conjugate, $b^{-1}ab = a$ for any element b in G. Thus $(b^{-1}ab)^{p^{i-1}} = a^{p^{i-1}}$ or by associativity, $b^{-1}a^{p^{i-1}}b = a^{p^{i-1}}$ and hence $a^{p^{i-1}}$ is a self-conjugate element of order p. This proves the theorem.

COROLLARY 1: The number of self-conjugate elements in G is a positive power of p.

Proof: Since the set S of self-conjugate elements of G is a subset of G by lemma 1 it is necessary only to show closure of S to prove that it forms a subgroup of G. Let a and b be any two self-conjugate elements of G, and c be any element of G. Now $c^{-1}ac = a$ and $c^{-1}bc = b$. Therefore $(c^{-1}ac)(c^{-1}bc) = ab$

or by associativity and the definition of the identity and inverse elements, $c^{-1}abc = ab$. This establishes closure. It was shown in the theorem that S contains an element other than the identity. Therefore the number of elements of S is a positive power of p.

Note that Definition c and Corollary 1 imply that the center of a prime-power group G is greater than {e}.

COROLLARY 2: A group G of order p^2 is Abelian.

Proof: If G contains an element of order p^2 it is cyclic and hence Abelian. If G is not cyclic let a be a self-conjugate element of G of order p and let b be an element of G not in {a}. Then $b^{-1}ab = a$ or $ab = ba$. Since G is of order p^2 the elements b and a generate G.

COROLLARY 3: Every group G whose order is a multiple of a power of a prime p contains an element of order p.

Proof: Let G be of order kp^m. Then by Theorem b, G contains a subgroup of order p^m which by the previous theorem contains an element of order p.

THEOREM 3: In any group G of order p^m there exists a series of subgroups or orders $p, p^2, p^3, \ldots, p^{m-1}, p^m$, such that each is normal in G and in all the subgroups of the series which follow it.

Proof: By Theorem 2 there is an element of order p in G which is self-conjugate. Denote this element by a_1. By the process used in Corollary 1 and by Definition b it can be shown that $\{a_1\}$ is a normal subgroup of G. It is of order p. Denote this normal subgroup by H_1. Consider the factor group G/H_1 (Definition f). It will be recalled that in this group the identity element is H_1 and its order is equal to the index of H_1 in G. Thus it is of order p^{m-1}.

Set up the natural homomorphism (Definition g) of $G \rightarrow G/H_1$ where the p elements of H_1 in G correspond to the identity element H_1 in G/H_1. Note that the element a is in H_1 if and only if $a \rightarrow H_1$. Since G/H_1 is of order p^{m-1}, it is a prime-power group and hence contains an element of order p which is self-conjugate. Denote this element by b_2. Let a_2 be one of the elements in G which corresponds to b_2. From the operation preserving property of homomorphisms, $a_2 \rightarrow b_2$ implies that $a_2^p \rightarrow b_2^p = H_1$. Thus a_2^p is in H_1. Let a be any element of G and b the corresponding element of G/H_1. Since b_2 is self-conjugate, $b^{-1}b_2b = b_2$ or $b_2^{-1}b^{-1}b_2b = e = H_1$ and therefore $a_2^{-1}a^{-1}a_2a$ is in H_1. It will now be shown that the set of elements $\{a_1, a_2\}$ forms a normal subgroup of G of order p^2. Denote this set of elements by H_2. That H_2 is closed follows from the fact that it is the set of elements made up of all possible products of powers of a_1 and a_2. Thus by Lemma 1, H_2 is a subgroup of G. If c is an arbitrary element of H_2 and a an arbitrary element of G, then $c^{-1}a^{-1}ca = a_1^{\,i}$ where $0 \leq i \leq p$. This then becomes $a^{-1}ca = ca_1^{\,i}$. However $ca_1^{\,i}$ is an element of H_2 by closure of H_2. Thus $a^{-1}H_2a = H_2$ and H_2 is a normal subgroup of G. The p^2 elements $a_1^{\,t_1}a_2^{\,t_2}(t_1, t_2 = 1, 2, \ldots, p)$ are distinct for $a_1^{\,x}a_2^{\,y} = a_1^{\,u}a_2^{\,v}$ implies that $a_2^{\,y-v} = a_1^{\,u-x}$, which says that $a_2^{\,y-v}$ is in H_1.

If $m > 2$ continue as before considering the factor group G/H_2. Since H_2 is of order p^2 the order of G/H_2 is p^{m-2}. Set up the homomorphism $G \rightarrow G/H_2$ where the p^2 elements of H_2 correspond to the identity element H_2 of G/H_2. Since G/H_2 is a prime-power group it contains a self-conjugate element of order p which will be denoted by b_3. Let a_3 be one of the elements of G which corresponds to b_3. This implies that $a_3^p \rightarrow b_3^p$ and $b_3^p = H_2$. Hence a_3^p is in H_2. Let a be any element of G and b an element of G/H_2 such that $a \rightarrow b$. Since b_3 is self-conjugate in G/H_2, $b^{-1}b_3b = b_3$ or $b_3^{-1}b^{-1}b_3b = e = H_2$ and thus $a_3^{-1}a^{-1}a_3a$ is in H_2. Let $H_3 = \{a_1, a_2, a_3\}$. Now H_3 is closed since it is made up of all possible products of powers of a_1, a_2, and a_3. Therefore by Lemma 1 it is a subgroup of G. Let c be an arbitrary element of H_3 and a an arbitrary element of G. Then $c^{-1}a^{-1}ca = a_1^i a_2^j$ where $0 \leq i, j \leq p$. This is equivalent to $a^{-1}ca = ca_1^i a_2^j$. By closure of H_3 this becomes $a^{-1}H_3a = H_3$ and H_3 is a normal subgroup of G. The p^3 elements

$a_1^{t_1}a_2^{t_2}a_3^{t_3}(t_1, t_2, t_3 = 1, 2, \ldots, p)$ are distinct for $a_1^x a_2^y a_3^z = a_1^u a_2^v a_3^w$ implies that $a_3^{z-w} = a_1^{u-x}a_2^{v-y}$ which says that a_3^{z-w} is in H_2.

Now consider the factor group G/H_3 and take a self-conjugate element b_4 of order p in G/H_3 and proceed as before if $m > 3$. The process can be continued until one obtains the p^m elements $a_1^{t_1}a_2^{t_2}\ldots a_m^{t_m}(t_i = 1, 2, \ldots, p;$

$i = 1, 2, \ldots, m$). In general then b_i is a self-conjugate element of order p in G/H_{i-1} where $H_i = \{a_1, a_2, \ldots, a_i\}$. In the homomorphism $G \rightarrow G/H_{i-1}$, a_i in G is chosen such that $a_i \rightarrow b_i$. Then H_i forms a normal subgroup of G of order p^i. The normality of H_i follows directly from the fact that for any element a of G, $a_i^{-1}a^{-1}a_i a$ and a_i^p are in H_{i-1}. The p^i are all distinct because for all i, $a_1^{x_1}a_2^{x_2}\ldots a_i^{x_i} = a_1^{u_1}a_2^{u_2}\ldots a_i^{u_i}$ implies that $a_i^{x_i-u_i} = a_1^{u_1-x_1}a_2^{u_2-x_2}\ldots a_{i-1}^{u_{i-1}-x_{i-1}}$ which says that $a_i^{x_i-u_i}$ is in H_{i-1}. Since all products of powers of the a_i's are elements of G by closure of G, and since all p^m of them are distinct it follows that every element of G is included once and only once among the p^m elements $a_1^{t_1}a_2^{t_2}\ldots a_m^{t_m}$ ($t_i = 1, 2, \ldots, p$; $i = 1, 2, \ldots, m$). It was shown that every H_i is a normal subgroup of G. From the nature of the H_i's it is apparent that every H_i is a subgroup of H_{i+s} where $1 \leq s \leq m-i$. Since H_i is normal in G, $a^{-1}H_i a = H_i$ for any element a of G. This is also true whenever a is an element of H_{i+s} and thus any one of the subgroups $H_1, H_2, \ldots, H_{m-1}, H_m = G$ of order $p, p^2, \ldots, p^{m-1}, p^m$ is normal in all the subgroups succeeding it.

The following corollary was proven in the course of the theorem.

COROLLARY 1: A group G of order p^m contains a set of elements $a_1, a_2, \ldots, a_m$ such that a_i^p and $a_i^{-1}a^{-1}a_i a$ (where a is any element of G) are in the group $H_{i-1} = \{a_1, a_2, \ldots, a_{i-1}\}$ for $i = 1, 2, \ldots, m$, while H_i consists

of the p^i elements $a_1^{t_1}a_2^{t_2}\ldots a_i^{t_i}(t_k = 1, 2, \ldots, p;\ k = 1, 2, \ldots, i)$.

THEOREM 4: Every subgroup H of order p^s in a group G of order p^m is contained normally in a subgroup of order p^{s+1} where $0 \leq s < m$.

Proof: Use the notation of Theorem 3. If H does not contain a_1, then it will be shown that $\{H, a_1\}$ is the subgroup required. Since this is generated by a subgroup and an element of G it is necessarily closed and is hence a subgroup of G by Lemma 1. By closure $Ha_1^j = a_1^jH$ and $Hh = hH$ where $1 \leq j \leq p$ and h is an element of H. Therefore $(a_1^j)^{-1}Ha_1^j = H$ and $h^{-1}Hh = H$ which proves that H is normal in $\{H, a_1\}$. Since a_1 is of order p, $\{H, a_1\} = H \cup Ha_1 \cup Ha_1^2 \cup \ldots \cup Ha_1^{p-1}$ and is hence of order p^{s+1}. If H contains $a_1, a_2, \ldots, a_{i-1}$ but does not contain a_i it will be shown that $\{H, a_i\}$ is the required subgroup. Again by Lemma 1 this is a subgroup of G. Now $a_i^{-1}h^{-1}a_ih$ is in H_{i-1} by Corollary 1 of Theorem 3 and hence in H since $H_{i-1} \subseteq H$. This says by closure of H that $(a_i^{-1})^jHa_i^j = H_{i-1}h^{-j} = H$ and again $h^{-1}Hh = H$. Therefore since $(a_i^{-1})^j = (a_i^j)^{-1}$ the normality is established. Now a_i^p is in H_{i-1} by Corollary 1 of Theorem 3 and is hence in H. Therefore $\{H, a_i\} = H \cup Ha_i \cup Ha_i^2 \cup \ldots \cup Ha_i^{p-1}$ and is of order p^{s+1}.

In particular taking $s = m - 1$ the following corollary results.

COROLLARY 1: Every subgroup H of order p^{m-1} in a group G of order p^m is normal in G.

NUMBER OF SUBGROUPS OF A GIVEN ORDER

LEMMA 2: The number of subgroups of order p^s in a group G of order p^m where G is Abelian of type (1, 1, ..., 1) is equal to

$$\frac{(p^m - 1)(p^m - p)(p^m - p^2)\ldots(p^m - p^{s-1})}{(p^s - 1)(p^s - p)(p^s - p^2)\ldots(p^s - p^{s-1})} .$$

Proof: By Definition h all elements of G other than the identity are of order p. Hence a subgroup of order p^s is of type (1, 1, ..., 1) also but in this case with s 1's. By Theorem e, a subgroup of G of order p^s has s generators of order p. The first generator a_1 can be chosen from G in $p^m - 1$ different ways. The group a_1 contains p - 1 elements of order p. Hence there remain $(p^m - 1) - (p - 1) = p^m - p$ elements of order p so that the second generating element a_2 can be chosen in $p^m - p$ different ways. The group $\{a_1, a_2\}$ contains $p^2 - 1$ elements of order p so that the remaining elements of order p are $(p^m - 1) - (p^2 - 1) = p^m - p^2$ in number. Thus the third generating element can be obtained in $p^m - p^2$ different ways. In the same manner the fourth generating element can be chosen in $p^m - p^3$ different ways. The process is continued until the sth and final generating element may be chosen in $p^m - p^{s-1}$ different ways. Hence the number of choices of the ordered set of s generators which give rise to a subgroup of order p^s is $(p^m - 1)(p^m - p)(p^m - p^2)\ldots(p^m - p^{s-1})$. By the same method an ordered set of generators of a given group of order p^s and type (1, 1, ..., 1) may be selected in $(p^s - 1)(p^s - p)(p^s - p^2)\ldots(p^s - p^{s-1})$ different ways since this group has

s generating elements. Therefore the number of subgroups of G of order p^s is the quotient of these two numbers and the lemma is proven.

THEOREM 5: If p^d is the order of the greatest common subgroup D of the subgroups of order p^{m-1} in a group G of order p^m, G contains $(p^{m-d} - 1)/(p - 1)$ subgroups of order p^{m-1}.

Proof: Let $H_1, H_2, \ldots, H_r$ be the subgroups of G of order p^{m-1} and hence of index p. Then by Corollary 1 of Theorem 4, each H_i is normal in G. Set up the homomorphism $G \rightarrow G/H_i$ and the homomorphism $G \rightarrow G/D$. Let a be an arbitrary element of G, b_i the corresponding element of G/H_i and b the corresponding element of G/D. Since each H_i is of order p^{m-1}, G/H_i is of order p and hence $b_i^p = e$, where e is the identity element of G/H_i, for all i = 1, 2, ..., r. Therefore a^p is in H_i for each value of i and a^p is in D. Thus note that D contains the pth power of every element of G since a is arbitrary. Since a^p is in D, the corresponding element b^p is the identity element of G/D. Each G/H_i is of order p and hence Abelian by Corollary 2 of Theorem a. Therefore by Corollary 2 of Theorem g, H_i contains the commutator subgroup Δ of G. Thus D contains Δ. By Corollary 1 of Theorem g, G/D is Abelian. Since it is always true that $b^p = e$ for any element a of G to which b corresponds, it follows that every element of G/D is of order 1 or p. Thus G/D is of type $(1, 1, \ldots, 1)$. The order of D is p^d and hence the order of G/D is p^{m-d}. By Lemma 2, G/D contains $(p^{m-d} - 1)/(p - 1)$ subgroups of index p. By the homomorphism $G \rightarrow G/D$, to each subgroup of index p in G/D there corresponds one and

only one subgroup of index p in G. Therefore the number of subgroups of index p in G/D is the same as the number of subgroups of index p in G. Therefore the number of subgroups of index p in G is $(p^{m-d} - 1)/(p - 1)$.

The following corollaries were proven in the proof of the theorem.

COROLLARY 1: The pth power of every element of G of order p^m is in D.

COROLLARY 2: The group G/D is Abelian of order p^{m-d} and type (1, 1, ..., 1) where d is the order of D.

It will be noted that if G is Abelian of type (1, 1, ..., 1) the only element common to the subgroups of G of order p^{m-1} is the identity of G. Thus D is of order $p^0 = 1$ and d = 0. Therefore the number of subgroups of order p^{m-1} in G is $(p^m - 1)/(p - 1) = p^{m-1} + p^{m-2} + \ldots + p + 1$. This proves the following corollary.

COROLLARY 3: If G is Abelian of order p^m and of type (1, 1, ..., 1) the number of subgroups of order p^{m-1} is $p^{m-1} + p^{m-2} + \ldots + p + 1$.

COROLLARY 4: The number of subgroups of order p^{m-1} in a group of order p^m is congruent to one modulo p.

Proof: This corollary becomes apparent when it is noted that $(p^{m-d} - 1)/(p - 1) = p^{m-d-1} + p^{m-d-2} + \ldots + p + 1$.

THEOREM 6: The number of subgroups of order p^s in a group G of order p^m is of the form 1 + kp where k is a non-negative integer.

Proof: By Theorem h the number of subgroups conjugate to a subgroup H of G is equal to the index of the normalizer K (Definition j) of H in G. However any subgroup of G is of order a non-negative power of p and hence the index of K is a non-negative power of p. If H is not normal in G, then $K \neq G$

and the index of K is a positive power of p. Thus the number of subgroups conjugate to any subgroup not normal in G is a multiple of p. For a particular subgroup of order p^s which is not normal in G, there are associated with it those subgroups conjugate to it. This set of conjugate subgroups (including the particular one in question) is a multiple of p in number. Each subgroup conjugate to a group of order p^s is also of order p^s. Therefore the number of subgroups of order p^s not normal in G is congruent to 0 mod p. It thus suffices to show that the number of subgroups of order p^s normal in G is congruent to 1 mod p to prove the theorem.

By Theorem 3, G contains at least one normal subgroup of order p^s. Denote the subgroups of order p^s normal in G by $H_1, H_2, \ldots, H_t$. Let $K_1, K_2, \ldots, K_r$ be the subgroups of G of order p^{m-1}. By Corollary 1 of Theorem 4 these are all normal in G. By Corollary 4 of Theorem 5 the number of these is congruent to 1 mod p. That is $r \equiv 1 \bmod p$. It suffices to show that $t \equiv 1 \bmod p$. Let a_i be the number of subgroups $H_1, H_2, \ldots, H_t$ which are in K_i where $i = 1, 2, \ldots, r$. Let b_j be the number of subgroups $K_1, K_2, \ldots, K_r$ each of which contains H_j where $j = 1, 2, \ldots, t$. Then the number of cases in which a group of order p^s is in a group of order p^{m-1} is $a_1 + a_2 + \ldots + a_r$. The number of cases in which a group of order p^{m-1} contains a group of order p^s is $b_1 + b_2 + \ldots + b_t$. Thus $a_1 + a_2 + \ldots + a_r = b_1 + b_2 + \ldots + b_t$. The subgroups of G of order p^{m-1} containing a given subgroup H_j are the subgroups of G corresponding to subgroups of index p in the homomorphism $G \rightarrow G/H_j$.

The number of subgroups of index p in G/H_j is congruent to one modulo p by Corollary 4 of Theorem 5. Thus $b_j \equiv 1 \bmod p$. Therefore $a_1 + a_2 + \ldots + a_r \equiv 1 + 1 + \ldots + 1 \bmod p$ or equivalently $a_1 + a_2 + \ldots + a_r \equiv t \bmod p$. By Corollary 1 of Theorem 4 and Corollary 4 of Theorem 5 the number of normal subgroups of order p^s in any given group of order p^{s+1} is congruent to one modulo p. It will be assumed that the same is true for groups of orders p^{s+2}, p^{s+3}, ..., p^{m-1}, and by induction prove it true for the group G of order p^m. By the assumption the number of normal subgroups of order p^s contained in K_i is congruent to one modulo p. These subgroups include the a_i subgroups contained in K_i and normal in G and certain other subgroups $L_1, L_2, \ldots, L_u$ of order p^s which are normal in K_i but not normal in G. Since K_i is normal in G, K_i contains every subgroup conjugate to any of the groups $L_1, L_2, \ldots, L_u$. Hence as in the beginning of the proof of this theorem, $u \equiv 0 \bmod p$. Therefore $a_i \equiv 1 \bmod p$. Thus $a_1 + a_2 + \ldots + a_r \equiv r \bmod p$. Combining this with the previously shown fact $a_1 + a_2 + \ldots + a_r \equiv t \bmod p$, $t \equiv r \bmod p$ is obtained. It was shown that $r \equiv 1 \bmod p$ and hence $t \equiv 1 \bmod p$ and the theorem is proven.

It is now possible to prove the following theorem which is an extension, of a sort, of Sylow's Theorem (Theorem b) and is due to Frobenius.

THEOREM 7: If G is any group whose order is divisible by a prime-power p^s $(s > 0)$, then the number of subgroups of order p^s in G is of the form $1 + kp$.

Proof: Let p^m be the highest power of p contained as a factor in the order of G. By Theorem b there exists a subgroup of order p^m contained in G.

Call it G_1. If a given subgroup of G of order p^s is not normal in G, then by the first part of the proof of Theorem 6 it is transformed by the elements of G_1 into a set of conjugates whose number is a power of p and hence this number is congruent to 0 mod p. By Theorem 6, the number of normal subgroups of order p^s of G is congruent to 1 mod p. Thus the number of subgroups of G of order p^s is congruent to 1 mod p or is of the form $1 + kp$.

PRIME-POWER GROUPS CONTAINING ONE SUBGROUP OF A GIVEN ORDER

LEMMA 3: In a group G if $b^{-1}ab = a^n$, then $b^{-r}ab^r = a^{n^r}$ where a and b are elements of G, n is a given fixed positive integer less than the order of a, and r is any positive integer.

Proof: If $r = 1$, the conclusion and hypothesis are identical equations. It will first be shown that the lemma is true if $r = 2$. Since $b^{-1}ab = a^n$, $(b^{-1}ab)^n = (a^n)^n$. This is equivalent to $b^{-1}a^nb = a^{n^2}$. Thus by substitution for a^n, $b^{-1}(b^{-1}ab)b = a^{n^2}$ and $b^{-2}ab^2 = a^{n^2}$. Now assume the statement to be true for $r - 1$. Now $b^{-1}ab = a^n$ implies that $(b^{-1}ab)^{n^{r-1}} = (a^n)^{n^{r-1}}$ which is equivalent to $b^{-1}a^{n^{r-1}}b = a^{n^r}$. By the induction hypothesis, $a^{n^{r-1}} = b^{-(r-1)}ab^{r-1}$ in which case it follows that $b^{-r}ab^r = a^{n^r}$ and the lemma is proven by induction.

LEMMA 4: If a group G of order p^m contains only one subgroup G_s of order p^s, where s is a given positive integer less than m, then G_s is a cyclic group and any element a of G not contained in G_s is of order p^{s+t} where t is a positive integer.

Proof: Let a be the element of G not contained in G_s. Assume that the order of a is less than p^{s+1}. Let the order of the element a be p^{s_1}. Then $0 < s_1 \leq s$ since $a^0 = e$ would have to be in G_s. The group $\{a\}$ is a subgroup of G of order p^{s_1} and is contained in a subgroup of G of order p^{s_1+1} which in turn is contained in a subgroup of G of order p^{s_1+2}, and hence by repeated application of Theorem 4, $\{a\}$ is contained in a subgroup of G of order p^s. This subgroup obviously contains the element a and hence is not G_s. However by the hypothesis G_s is the only subgroup of G of order p^s. Thus the assumption that the order of a is less than p^{s+1} is false and the order of a is p^{s+t} where t is a positive integer. Hence $a^{p^{s+t}} = e$ and this is the smallest positive power of a such that this is true. However $a^{p^{s+t}} = (a^{p^t})^{p^s}$ and hence a^{p^t} is of order p^s and generates a subgroup G of order p^s. Thus by the hypothesis of the theorem the cyclic group $\{a^{p^t}\}$ must coincide with G_s and G_s is a cyclic group.

LEMMA 5: Let G_r be a subgroup of G where G_r is the only subgroup of G of order p^r and G is of order p^m $(0 < r < m)$. Let G_{r+1} be a non-cyclic subgroup of G where G_{r+1} is of order p^{r+1}. Let G_r be contained normally in G_{r+1}. Then if b_1 is an element of G_{r+1} not contained in G_r there exists a positive integer g and a non-negative integer k which is prime to p such that $b_1^p = b^{gp}$ and $b_1^{-1} b b_1 = b^{1+kp^{r-1}}$ where b is a generating element of G_r.

Proof: By Lemma 4, G_r is cyclic and hence contains a generating element b of order p^r. Since b_1 is an element of G_{r+1} which is not contained in G_r and G_r is a normal subgroup of G_{r+1} there exist positive integers i and j such that $b_1^{-1}bb_1 = b^i$ and $b_1^p = b^j$. Assume that j is not divisible by p. Then the order of b^j would be p^r since $G_r = \{b\}$ is cyclic and of order p^r. This says that b_1^p is of order p^r which says that b_1 is of order p^{r+1} since $(b_1^p)^{p^r} = b_1^{p^{r+1}} = e$ and this is the least positive power of b_1 such that this is true. However since G_{r+1} is not cyclic, b_1 cannot be of order p^{r+1}. Hence $j = gp$ where g is a positive integer. This proves the first part of the lemma.

Let b_1^q be the least positive integral power of b_1 such that b_1^q is permutable with b. Thus $b_1^{-q}bb_1^q = b$. By Lemma 3, the relation $b_1^{-1}bb_1 = b^i$ implies that $b_1^{-q}bb_1^q = b^{i^q}$. Therefore $b^{i^q} = b$ and $i^q \equiv 1 \bmod p^r$ since $b^{p^r} = e$. By Theorem i, in the group $\{b, b_1\}$ the element b is one of a complete set of q conjugates and q is a positive power of p. Since $b_1^p = b^j$, $b^{-j}bb^j = b$ implies that $b_1^{-p}bb_1^p = b$ and hence $q \leq p$. Since q is a positive power of p, $p = q$. Thus $i^p \equiv 1 \bmod p^r$. Assume that $i \equiv 1 \bmod p^r$. Then $b_1^{-1}bb_1 = b$ and the group $\{b, b_1\}$ would be Abelian of type (r, 1) since b is of order p^r and b_1 is in G_{r+1} implying that b_1 would have to be of order p by theorem e. This group would then contain an element b_1 of order p and not occurring in $\{b\}$.

By Lemma 4 if b_1 is not in G_r its order must be p^{r+t} where t is a positive integer. Thus a contradiction is reached from the assumption that $i \equiv 1 \bmod p^r$ and hence $i \not\equiv i \bmod p^r$. However $i^p \equiv i \bmod p$ for all positive integral i by Theorem j. It has also been shown that $i^p \equiv 1 \bmod p^r$. Thus $i \equiv 1 \bmod p$. Hence i is of the form $i = 1 + kp^u$ where u is chosen so that k is prime to p. (i.e. all powers of p are factored out of h if $i \equiv 1 \bmod p$ were written as $i = 1 + hp$.) Note that u may be equal to one. It is less than r since $i \not\equiv 1 \bmod p^r$. It is greater than 0 by definition of congruence. Now

$$i^p = (1 + kp^u)^p = 1 + kp^{u+1} + \tfrac{1}{2}p(p - 1)k^2p^{2u} + \ldots + k^pp^{pu}.$$

By noting that p^{u+1} divides all terms of the expansion except the first and that $i^p \equiv 1 \bmod p^r$ it is apparent that $u = r - 1$. Thus $b_1^{-1}bb_1 = b^{1+kp^{r-1}}$.

LEMMA 6: If a and b are two elements of a group G of order p^m and are such that $b^{-1}ab = a^n$ where n is a given positive integer, then for any integral x and for all positive integral r, $(a^xb)^r = b^ra^{x(n+n^2+\ldots+n^r)}$.

Proof: The hypothesis $b^{-1}ab = a^n$ implies that $(b^{-1}ab)^x = (a^n)^x$ which is equivalent to $b^{-1}a^xa = a^{nx}$ or $a^xb = ba^{nx}$. Now

$$\begin{aligned}
b^{-r}(a^xb)^r &= b^{1-r}(b^{-1}a^xb)(a^xb)^{r-1} \\
&= b^{1-r}(a^{nx})(a^xb)^{r-1} \\
&= b^{2-r}\left[b^{-1}a^{x(n+1)}b\right]\left[a^xb\right]^{r-2} \\
&= b^{2-r}\left[a^{x(n^2+n)}\right]\left[a^xb\right]^{r-2} \\
&= b^{3-r}\left[b^{-1}a^{x(n^2+n+1)}b\right]\left[a^xb\right]^{r-3}
\end{aligned}$$

$$= b^{3-r}\left[a^{x(n^3+n^2+n)}\right]\left[a^{x}b\right]^{r-3}$$

$$= b^{-1}\left[a^{x(n^{r-1}+n^{r-2}+\ldots+n+1)}\right]b$$

$$= a^{x(n^r+n^{r-1}+\ldots+n^2+n)}.$$

Therefore $(a^x b)^r = b^r a^{x(n+n^2+\ldots+n^r)}$ which proves the lemma.

THEOREM 8: If a group G of odd order p^m contains only one subgroup G_s of order p^s, where s is a given positive integer less than m, then G is a cyclic group.

Proof: Let p^r be the largest number which is the order of an element of G and let b be an element of G which is of order p^r. Then $\{b\}$ is either identical with G or by Theorem 4 is contained normally in a subgroup G_{r+1} of order p^{r+1}. In the first case where r = m, G is cyclic and the theorem is proven. In the second case G_{r+1} is non-cyclic since $b^{p^r} = e$ and the other generator is of order p. It will be shown that the second case cannot exist.

Thus assume that $\{b\}$ is a normal subgroup of G_{r+1}. Let b_1 be an element of G_{r+1} which is not contained in $\{b\}$. Then by Lemma 5 there exists a non-negative integer k which is prime to p such that $b_1^{-1}bb_1 = b^{1+kp^{r-1}}$. Then applying Lemma 6, $(b^x b_1)^p = b_1^p b^{x(i+i^2+\ldots+i^p)}$ where x is any integer and $i = 1 + kp^{r-1}$. Now

$$i + i^2 + \ldots + i^p = (1 + kp^{r-1}) + (1 + kp^{r-1})^2 + \ldots + (1 + kp^{r-1})^p.$$

Since every term in which k is of degree 2 or greater of the expansion of this

equation is a multiple of p^r and b is of order p^r it becomes apparent that

$$(b^x b_1)^p = b_1^p b^{x\left[p+(1+2+\ldots+p)kp^{r-1}\right]} = b_1^p b^{x\left[p+\frac{1}{2}p(p+1)kp^{r-1}\right]}.$$

By hypothesis p is odd and hence $\frac{1}{2}(p+1)$ is a positive integer and $\frac{1}{2}(p+1)k$ is a positive integer h. Therefore $(b^x b_1)^p = b_1^p b^{x(p+hp^r)} = b_1^p b^{xp}$ since b is of order p^r. By Lemma 5 there exists a positive integer g such that $b_1^p = b^{gp}$. Taking $x = -g$ and using the last two equations yields $(b^{-g}b_1)^p = b_1^p b^{-gp} = e$. However $b^{-g}b_1$ is not in $\{b\}$. By Lemma 4, $b^{-g}b_1$ must be of order p^{r+1} or greater. Since it was just shown to be of order p or less a contradiction is reached and hence only the first alternative indicated earlier is possible and G is cyclic.

LEMMA 7: The solutions to the equation $a^2 \equiv 1 \bmod 2^r$ are $a \equiv \pm 1 \bmod 2^r$ and $a \equiv \pm 1 \bmod 2^{r-1}$ the latter of which is the same as $a \equiv \pm 1 + 2^{r-1} \bmod 2^r$.

Proof: If $a^2 \equiv 1 \bmod 2^r$ then $a^2 - 1 \equiv 0 \bmod 2^r$ or $a - 1 \equiv 0 \bmod 2^k$ and $a + 1 \equiv 0 \bmod 2^{r-k}$ where $0 \leq k \leq r$. Adding 2 to both sides of the first of the latter two equations yields $a + 1 \equiv 2 \bmod 2^k$. Let $h = \min(r - k, k)$. Then $a + 1 \equiv 0 \bmod 2^h$ and $a + 1 \equiv 2 \bmod 2^h$. Thus $2 \equiv 0 \bmod 2^h$ and 2^h divides 2. This means that k is equal to 0, 1, r - 1, or r. Considering all possibilities yields $a \equiv \pm 1 \bmod 2^r$ and $a \equiv \pm 1 \bmod 2^{r-1}$. This proves the first part of the theorem.

If $a \equiv \pm 1 \bmod 2^{r-1}$ when $a \equiv \pm 1 \bmod 2^r$, then $a = \pm 1 + 2^{r-1}j$ for some odd integer j. Hence $j = 2n + 1$ for some integer n. Thus $a = \pm 1 + (2n + 1)2^{r-1} = \pm 1 + 2^{r-1} + 2^r n$ and $a \equiv \pm 1 + 2^{r-1} \bmod 2^r$.

THEOREM 9: If a group G of order 2^m contains only one subgroup G_s of order 2^s, where s is a given positive integer greater than 1 and less than m, then G is a cyclic group. If G contains only one subgroup G_1 of order 2, then G is either a cyclic group or a group of the type defined by the relations

$$b^{2^{m-1}} = e, \quad a^2 = b^{2^{m-2}}, \quad a^{-1}ba = b^{-1} \qquad (m > 2).$$

Proof: As in Theorem 8 let 2^r be the largest number which is the order of an element of G and let b be an element of G which is of order 2^r. Then $\{b\}$ is either identical with G or by Theorem 4 is contained normally in a subgroup G_{r+1} of order p^{r+1}. In the first case where r = m the theorem is proven. In the second case G_{r+1} is non-cyclic since $b^{2^r} = e$ and the other generator is of order 2. It will be shown that the second case cannot exist if $s \geq 2$. This will prove the first part of the theorem.

Thus assume that $\{b\}$ is a normal subgroup of G_{r+1}. Let b_1 be an element of G_{r+1} which is not contained in $\{b\}$. Then by Lemma 5 there exists a non-negative integer k such that $b_1^{-1}bb_1 = b^{1+2^{r-1}k}$. Then applying Lemma 6, $(b^x b_1)^4 = b_1^4 b^{x(i+i^2+i^3+i^4)}$ where x is any integer and $i = a + 2^{r-1}k$. As in Theorem 8,

$$i + i^2 + i^3 + i^4 \equiv 4 + \tfrac{1}{2}(4)(4+1)2^{r-1}k \equiv 4 + (10k)(2^{r-1}) \equiv 4 \bmod 2^r.$$

Since b is of order 2^r it follows that $(b^x b_1)^4 = b_1^4 b^{4x}$. By Lemma 5 there exists a positive integer g such that $b_1^2 = b^{2g}$. Taking x = -g and using the last two equations yields $(b^{-g}b_1)^4 = b_1^4 b^{-4g} = e$. Thus $b^{-g}b_1$ is an element of

order at most 4 which is not contained in $\{b\}$. By Lemma 4, $b^{-g}b_1$ must be of order 2^{r+1} or greater. Since it was just shown to be of order 2^2 or less a contradiction is reached if $s \geq 2$ in which case G is cyclic and the first part of the theorem is proven.

Now consider the second part of the theorem in which case G has only one subgroup G_1 of order 2. By Theorem k the only group of order 2^2 containing only one subgroup of order 2 is the cyclic group. If $m = 2$, G_1 coincides with G. Thus G has been shown to be cyclic unless $m > 2$. Hence it will be assumed that $m > 2$. Let 2^r be the largest number which is the order of an element of G and let b be an element of G of order 2^r. As before if $r = m$, G_r and G coincide and the theorem is proven. Thus assume $r < m$. The group $\{b\}$ is a normal subgroup of a group G_{r+1} of order 2^{r+1} by Theorem 4. Let b_1 be an element of G_{r+1} of order as small as possible and such that it is not in $\{b\}$. Since the restrictions on b and b_1 are the same as in the first part of the proof with the additional restriction that b_1 is of minimum order, as before there exists a positive integer g such that $(b^{-g}b_1)^4 = e$ while $b^{-g}b_1$ is not in $\{b\}$. Hence $b^{-g}b_1$ is of order not greater than 4. Since it was assumed that b_1 is of minimum order consistent with the fact that it is in G_{r+1} and not in $\{b\}$ and since $b^{-g}b_1$ is in G_{r+1} and not in $\{b\}$ and of order not greater than 4, it follows that b_1 is of order not greater than 4. However if b_1 is of order less than 4 this contradicts the results of Lemma 4 since $\{b\}$ is of order 2^r and greater

than 2. Thus b_1 is of order 4 and b_1^2 is of order 2. Note that $(b^{2^{r-1}})^2 = e$ and since b is of order 2^r, $b^{2^{r-1}}$ is of order 2. By hypothesis G contains only one subgroup of order 2. Hence $b^{2^{r-1}} = b_1^2$ and b_1^2 is in $\{b\}$. Since $\{b\}$ is a normal subgroup of G_{r+1} there exists a positive integer i such that $b_1^{-1}bb_1 = b^i$. By Lemma 3, $b_1^{-2}bb_1^2 = b^{i^2}$. Since b_1^2 is in $\{b\}$, b and b_1^2 are permutable and $b_1^{-2}bb_1^2 = b$. Thus $b^{i^2} = b$. Therefore $i^2 \equiv 1 \bmod 2^r$. This is true because b is of order 2^r. By Lemma 7 the only solutions to this equation are $i \equiv \pm 1 \bmod 2^r$ and $i \equiv \pm 1 + 2^{r-1} \bmod 2^r$. If $i \equiv 1 \bmod 2^r$, then $b_1^{-1}bb_1 = b$ and $\{b, b_1\}$ would be Abelian of type (r, 1) and would hence contain the element b_1 of order 2 and not in $\{b\}$. This contradicts Lemma 4.

If $i \equiv \pm 1 + 2^{r-1} \bmod 2^r$, then $b_1^{-1}bb_1 = b^{\pm 1+2^{r-1}}$. Taking r to be greater than one and raising both sides of the equation to the 2^{r-1} power yields

$$b_1^{-1}b^{2^{r-1}}b_1 = b^{\pm 2^{r-1}+2^{2r-2}} = b^{\pm 2^{r-1}}$$

since b is of order 2^r and $2r - 2 \geq r$ when $r > 1$. However since $b^{2^{r-1}}$ is its own inverse it follows that $b^{2^{r-1}} = b^{-2^{r-1}}$ so that in either case $b_1^{-1}b^{2^{r-1}}b_1 = b^{2^{r-1}}$ which says that the group $\left\{b_1, b^{2^{r-1}}\right\}$ is a non-cyclic Abelian group. It is obviously a subgroup of G since b_1 and b are elements of G. Since in this case $\{b_1\}$ and $\left\{b^{2^{r-1}}\right\}$ are subgroups of G of order 2 by

Theorem e, there is more than one subgroup of G of order 2. This contradicts the hypothesis of the theorem and hence $i \not\equiv \pm 1 + 2^{r-1} \bmod 2^r$. Thus $i \equiv -1 \bmod 2^r$. Hence $b_1^{-1} b b_1 = b^{-1}$ when $r > 1$. If $r = 1$, $b_1^{-1} b b_1 = b^{\pm 1 + 2^{r-1}}$ implies that $b_1^{-1} b b_1 = e$ since in this case $b^2 = e$. This implies that $b = e$ and hence $r \neq 1$.

It is now necessary to show that $r = m - 1$. It will be remembered that the case being considered here is $r < m$. Hence now it will be assumed that $r < m - 1$ and then a contradiction to this assumption will be reached proving that $r = m - 1$. Since b is of order 2^r and b_1^2 is in $\{b\}$, $\{b, b_1\}$ is of order 2^{r+1}. Hence by Theorem 4 it is contained normally in a subgroup of G of order 2^{r+2}. Let b_2 be an element of this subgroup G_{r+2} such that b_2 is not contained in $\{b, b_1\}$. Since $\{b, b_1\}$ is contained normally in G_{r+2} it follows that $b_2^{-1}\{b, b_1 b_2\} = \{b, b_1\}$. However it is also true that $b_2^{-1}\{b\}b_2 = \{b\}$, for if this were not true then there would exist some positive integer t such that $b_2^{-1} b^{2^{r-1}} b_2 = b_1 b^t$, remembering that b_1^2 is in $\{b\}$. Squaring both sides of the equation yields $(b_1 b^t)^2 = b_2^{-1} b^{2^r} b_2 = e$. Note that this is the least positive power of $b_1 b^t$ such that this is true. Hence $\{b_1 b^t\}$ is of order 2 and $\{b^{2^{r-1}}\}$ is of order 2. Since G contains only one subgroup of order 2, $b_1 b^t = b^{2^{r-1}}$ which says that $b_1 = b^{2^{r-1}-t}$. This is a contradiction since b_1 is not in $\{b\}$.

Since b_2 and b are in G_{r+2}, the group $\{b, b_2\}$ is of order not greater than 2^{r+2}. Since b is of order 2^r, b_2^4 must be in $\{b\}$. Now assume that b_2^2 is in $\{b\}$. Then b_2^2 and b are permutable. Recall that in an earlier part of the theorem it was shown that b_1^2 and b permutable along with $b_1^{-1}\{b\}b_1 = b$ imply that $b_1^{-1}bb_1 = b^{-1}$. In an exactly analoguous manner then $b_2^{-1}bb_2 = b^{-1}$. Thus $b_1^{-1}bb_1 = b_2^{-1}bb_2$ which is equivalent to $b = b_1b_2^{-1}bb_2b_1^{-1}$. This says that b and $b_2b_1^{-1}$ are permutable and hence that $\{b, b_2b_1^{-1}\}$ is a non-cyclic Abelian group. Since b, b_1, and b_2 are in G_{r+2}, the group $\{b, b_2b_1^{-1}\}$ is of order at most 2^{r+2}. Since b is of order 2^r, $\{b, b_2b_1^{-1}\}$ is of order not less than 2^r. It is not of order 2^r for if it were, $b_2b_1^{-1} = b^w$ for some non-negative integer w. This implies that $b_2 = b^wb_1$ which cannot be true since b_2 was so chosen that b_2 is not an element of $\{b, b_1\}$. If $\{b, b_2b_1^{-1}\}$ is of order 2^{r+1} then $\{b_2b_1^{-1}\}$ is of order 2. However $\{b^{2^{r-1}}\}$ is also of order 2. Since G contains only one subgroup of order 2, $b^{2^{r-1}} = b_2b_1^{-1}$ or $b_2 = b^{2^{r-1}}b_1$ which is a contradiction since b_2 is not in $\{b, b_1\}$. If $\{b, b_2b_1^{-1}\}$ is of order 2^{r+2}, $\{b_2b_1^{-1}\}$ is of order 2^2 and $\{(b_2b_1^{-1})^2\}$ is of order 2. Again by the hypothesis of the theorem this implies that $(b_2b_1^{-1})^2$ is an element of $\{b\}$. If this is true, $\{b, b_2b_1^{-1}\}$ is of order 2^{r+1} which is a contradiction of the

assumption that $\{b, b_2 b_1^{-1}\}$ is of order 2^{r+2}. Hence in each case a contradiction is reached from the assumption that b_2^2 is in $\{b\}$. Now b_2^3 cannot be in $\{b\}$ for if it were then since $b_2^3 b_2 = b_2^4$ and b_2^4 is in $\{b\}$, this would imply by closure that b_2 is in $\{b\}$ contrary to assumption. Thus 4 is the least positive integral exponent of b_2 such that b_2 to this exponent is in $\{b\}$. Hence $\{b, b_2\}$ is of order 2^{r+2}. Now b_2^2 and b are not permutable for if they were then the Abelian group $\{b, b_2\}$ and hence G would contain the subgroups $\{b^{2^{r-1}}\}$ and $\{b_2^2\}$ of order 2 contrary to the hypothesis of the theorem.

Since $b_2^{-1}\{b\}b_2 = \{b\}$ there exists a positive integer j such that $b_2^{-1} b b_2 = b^j$. By Lemma 3, $b_2^{-2} b b_2^2 = b^{j^2}$ and $b_2^{-4} b b_2^4 = b^{j^4}$. Since b_2^2 and b are not permutable, $j^2 \not\equiv 1 \bmod 2^r$. Since b_2^4 is in $\{b\}$, b_2^4 and b are permutable so that $j^4 \equiv 1 \bmod 2^r$. By Lemma 7 the solutions of this congruence are $j^2 \equiv \pm 1 \bmod 2^r$ and $j^2 \equiv \pm 1 \bmod 2^{r-1}$. It has been shown that $j^2 \not\equiv 1 \bmod 2^r$. Now j^2 is an odd integer for if it were not then $b_2^{-2} b b_2^2 = b^{2k_1}$ for some positive integer k_1 or equivalently $b_2^{-2} b^{2^{r-1}} b_2^2 = b^{2^r k_1} = e$. Multiplying on the right by b_2^{-2} and the left by b_2^2 yields $b^{2^{r-1}} = e$ which is not true. Thus $j^2 + 1 \equiv 0 \bmod 2$. It is always true for any integer j that $j^2 \equiv 0 \bmod 4$ or $j^2 \equiv 1 \bmod 4$. Thus $j^2 + 1 \not\equiv 0 \bmod 4$. Hence j^2 is of the form $j^2 = -1 + 2k_2$

where k_2 is an odd integer. Thus $j^2 \not\equiv -1 \bmod 2^r$ and $j^2 \not\equiv -1 \bmod 2^{r-1}$. Therefore $j^2 \equiv 1 \bmod 2^{r-1}$ while $j^2 \not\equiv 1 \bmod 2^r$. Thus $j^2 = 1 + 2^{r-1}k_3$ where k_3 is an odd integer. Hence $b_2^{-2}b^2b_2^2 = (b^{1+2^{r-1}k_3})^2 = b^2$. Thus b_2^2 and b^2 are permutable and the group $\left\{b_2^2, b^2\right\}$ is Abelian with subgroups $\left\{b_2^2\right\}$ and $\left\{b^{2^{r-1}}\right\}$ of order 2. Thus G contains more than one subgroup of order 2 contrary to the hypothesis of the theorem. Thus the original assumption that $r < m - 1$ is false and $r = m - 1$. Hence it is now known that $b^{2^{m-1}} = e$, $a^2 = b^{2^{m-2}}$, and $a^{-1}ba = b^{-1}$, taking a to be b_1. It now remains to be shown that this group exists and is unique.

If this group does exist its elements are $b^u a^v$ where $u = 0, 1, \ldots, 2^{m-1}-1$ and $v = 0, 1$. If each element is multiplied on the left by b, another element of the set is obtained and in fact a determinate permutation of all the elements of the set is obtained, that permutation being

$$\rho = \begin{pmatrix} b^u a^v \\ b^{u+1} a^v \end{pmatrix}.$$

In like manner since $a^{-1}ba = b^{-1}$ implies that $ab = b^{-1}a$, it follows that

$$a(b^u a^v) = abb^{u-1}a^v = b^{-1}ab^{u-1}a^v = b^{-1}abb^{u-2}a^v = b^{-2}ab^{u-2}a^v.$$

After a total of u steps one has $a(b^u a^v) = b^{-u}a^{v+1}$. Hence multiplying each element on the left by a also yields another element of the set as well as a determinate permutation on the elements of the set, that being

$$\alpha = \begin{pmatrix} b^u a^v \\ b^{-u} a^{v+1} \end{pmatrix}.$$

(Associativity on the set has been assumed throughout although not specifically stated.) It contains the identity as has been determined. Hence if it is closed each element will contain an inverse so that closure remains to be shown to show that the set is a group. It is closed since each element is a product of powers of a and b and it is closed under multiplication on the left by a and b.

It now remains to show that this group is unique. The elements of any group G' determined by the hypothesis of the theorem must have the properties listed above and be of the form $a'^{u}b'^{v}$ where u = 0, 1, 2, ..., $2^{m-1} - 1$ and v = 0, 1 and where a' and b' are the generating elements of the group G'. However multiplying each element on the left by b' and a' respectively yields the respective permutations

$$\begin{pmatrix} b'^{u}a'^{v} \\ b'^{u+1}a'^{v} \end{pmatrix} \text{ and } \begin{pmatrix} b'^{u}a'^{v} \\ b'^{-u}a'^{v+1} \end{pmatrix}.$$

These are exactly the same permutations on the elements of G' which was obtained upon the elements of G. Hence if the set of permutations generated by ρ and α has the same properties as G and G' then this set will be a group isomorphic to G and G', and hence G and G' will be isomorphic to each other and abstractly identical. Hence note that

$$\rho^{2^{m-1}} = \begin{pmatrix} b^{u}a^{v} \\ b^{u+1}a^{v} \end{pmatrix}^{2^{m-1}} = \begin{pmatrix} b^{u}a^{v} \\ b^{u+2^{m-1}}a^{v} \end{pmatrix} = \begin{pmatrix} b^{u}a^{v} \\ b^{u}a^{v} \end{pmatrix}$$

which is the identity permutation. Also

$$\alpha^{2} = \begin{pmatrix} b^{u}a^{v} \\ b^{-u}a^{v+1} \end{pmatrix}^{2} = \begin{pmatrix} b^{u}a^{v} \\ b^{u}a^{v+2} \end{pmatrix} = \begin{pmatrix} b^{u}a^{v} \\ b^{u+2^{m-1}}a^{v} \end{pmatrix} = \rho^{2^{m-2}}.$$

Now note that

$$\alpha\beta^{-1} = \begin{pmatrix} b^u a^v \\ b^{-u} a^{v+1} \end{pmatrix} \begin{pmatrix} b^{u+1} a^v \\ b^u a^v \end{pmatrix} = \begin{pmatrix} b^u a^v \\ b^{-u-1} a^{v+1} \end{pmatrix}$$

and

$$\beta\alpha = \begin{pmatrix} b^u a^v \\ b^{u+1} a^v \end{pmatrix} \begin{pmatrix} b^u a^v \\ b^{-u} a^{v+1} \end{pmatrix} = \begin{pmatrix} b^u a^v \\ b^{-u-1} a^{v+1} \end{pmatrix}.$$

Therefore $\alpha\beta^{-1} = \beta\alpha$ or $\alpha^{-1}\beta\alpha = \beta^{-1}$. Thus $\{\beta, \alpha\}$ is a group isomorphic to G and to G' and hence G is unique. It now remains to show this group contains only one element of order 2. Since the order of b is 2^{m-1}, $z = 2^{m-2}$ is the only positive exponent of b less than 2^{m-1} such that $(b^z)^2 = e$. Thus if it can be shown that $(b^y a)^2 \neq e$ for any integral y such that $0 \leq y \leq 2^{m-1} - 1$, G contains only one element of order 2 remembering that $v = 0, 1$ and that $u = 0$ has been considered. Now

$$(b^y a)^2 = b^y a b^y a = b^{y-1}(ba)b^y a = b^{y-1} a b^{y-1} a$$

and after y steps this becomes $(b^y a)^2 = a^2 = b^{2^{m-2}} \neq e$. This proves the theorem.

PRIME-POWER GROUPS WITH A CYCLIC SUBGROUP OF INDEX p

THEOREM 10: If p is an odd prime and $m > 2$, there is one and only one abstract non-Abelian group G of order p^m containing an element of order p^{m-1}. It is the group defined by

$$a^p = b^{p^{m-1}} = e, \quad a^{-1} b a = b^{1+p^{m-2}}.$$

Proof: The reason for assuming $m > 2$ becomes apparent when it is noted that there are no non-Abelian groups of order p and p^2 by Corollary 2 of Theorem a and Corollary 2 of Theorem 2 respectively.

Assume that $m > 2$ and let b be an element of order p^{m-1} in a non-Abelian group G of order p^m if such a group exists. Since $\{b\}$ is cyclic and of order p^{m-1}, the element $b^{p^{m-2}}$ is in $\{b\}$ and is obviously the only element of $\{b\}$ of order p as $(b^{p^{m-2}})^p = b^{p^{m-1}} = e$. Thus $\{b\}$ contains only one subgroup of order p. Therefore G is non-Abelian and hence non-cyclic by the contrapositive statement of Corollary 2 of Theorem a. By the contrapositive statement of Theorem 8, when $s = 1$ it is seen that G non-cyclic implies that G contains more than one subgroup of order p. Thus G contains at least two elements of order p. There is only one such element in $\{b\}$ as was shown. Hence G contains an element b_1 of order p not contained in $\{b\}$. Now $\{b\}$ is normal in G by Corollary 1 of Theorem 4. This along with the fact that G is non-Abelian implies that there exists a positive integer i such that $b_1^{-1}bb_1 = b^i$ where $1 < i < p^{m-1}$. By Lemma 3 it follows that $b_1^{-p}bb_1^p = b^{i^p}$. However since b_1 is of order p it is true that $b_1^{-p}bb_1^p = b$. Thus $b = b^{i^p}$. Since b is of order p^{m-1}, $i^p \equiv 1 \bmod p^{m-1}$. This implies that $i^p \equiv 1 \bmod p$. By Theorem j, $i^p \equiv i \bmod p$. Hence $i \equiv 1 \bmod p$. Then i can be written as $i = 1 + kp^s$ where k is an integer and s is an integer chosen so that k is prime to p. Considering the definition of congruence and the fact that $i \not\equiv 1 \bmod p^{m-1}$, it is apparent that $0 < s < m - 1$.

Now

$$i^p = (1 + kp^s)^p = 1 + kp^{s+1} + \tfrac{1}{2}p(p-1)k^2p^{2s} + \ldots + k^pp^{ps}.$$

By noting that p^{s+1} divides all terms of the expansion except the first and that $i^p \equiv 1 \bmod p^{m-1}$ it is apparent that $s = m-2$. Thus $i = 1 + kp^{m-2}$. By Lemma 3, $b_1^{-x}bb_1^{x} = b^{i^x}$ for any integer x. Now

$$i^x = (1 + kp^{m-2})^x = 1 + kxp^{m-2} + \tfrac{1}{2}x(x-1)k^2p^{2m-4} + \ldots + k^xp^{mx-2x}.$$

Since $m > 2$, p^{m-1} divides all terms of the expansion of i^x except the first two. Hence since b is of order p^{m-1}, $b^{i^x} = b^{1+kxp^{m-2}}$. Let x be such that $kx \equiv 1 \bmod p$. Then

$$b^{i^x} = b^{1+(1+k_1p)p^{m-2}} = b^{1+p^{m-2}+k_1p^{m-1}} = b^{1+p^{m-2}}$$

where k_1 is an integer. Hence $b_1^{-x}bb_1^{x} = b^{1+p^{m-2}}$. Setting $a = b_1^{x}$ yields $a^{-1}ba = b^{1+p^{m-2}}$ where a is of order p since b_1 is of order p. Then the group $\{a, b\}$ satisfies the defining relations of the conclusion of the theorem provided this group exists. It is of order p^m. If this group exists its elements are a^ub^v where $u = 0, 1, 2, \ldots, p-1$ and $v = 0, 1, 2, \ldots, p^{m-1} - 1$. As in Theorem 9 it suffices only to show closure of the set by a multiplication of any element of the set by a and b in order to prove G a group. Also if this is done determinate permutations of the elements will be obtained, and if these permutations satisfy the previously determined properties satisfied by a and b this will suffice to show uniqueness of the group and will thus prove the theorem.

Multiplying $a^u b^v$ on the right by b yields $a^u b^{v+1}$. This determines the permutation

$$\beta = \begin{pmatrix} a^u b^v \\ a^u b^{v+1} \end{pmatrix}.$$

Since $a^{-1}ba = b^{1+p^{m-2}}$ is equivalent to $ba = ab^{1+p^{m-2}}$, multiplying on the right by a yields

$$a^u b^v a = a^u b^{v-1}(ba) = a^u b^{v-1} a b^{1+p^{m-2}} = a^u b^{v-2} a b^{2+2p^{m-2}}.$$

After v steps this becomes $a^u b^v a = a^{u+1} b^{v(1+p^{m-2})}$. The permutation determined is

$$\alpha = \begin{pmatrix} a^u b^v \\ a^{u+1} b^{v(1+p^{m-2})} \end{pmatrix}.$$

Thus G is a group. Now

$$\beta^{p^{m-1}} = \begin{pmatrix} a^u b^v \\ a^u b^{v+p^{m-1}} \end{pmatrix} = \begin{pmatrix} a^u b^v \\ a^u b^v \end{pmatrix}$$

which is the identity permutation and

$$\alpha^p = \begin{pmatrix} a^u b^v \\ a^u b^{v(1+p^{m-2})p} \end{pmatrix} = \begin{pmatrix} a^u b^v \\ a^u b^v \end{pmatrix}$$

which is also the identity permutation. Now

$$\beta\alpha = \begin{pmatrix} a^u b^v \\ a^u b^{v+1} \end{pmatrix} \begin{pmatrix} a^u b^v \\ a^{u+1} b^{v(1+p^{m-2})} \end{pmatrix} = \begin{pmatrix} a^u b^v \\ a^{u+1} b^{(v+1)(1+p^{m-2})} \end{pmatrix}$$

and

$$\alpha\beta^{1+p^{m-2}} = \begin{pmatrix} a^{u}b^{v} \\ a^{u+1}b^{v(1+p^{m-2})} \end{pmatrix} \begin{pmatrix} a^{u}b^{v} \\ a^{u}b^{v+1+p^{m-2}} \end{pmatrix} = \begin{pmatrix} a^{u}b^{v} \\ a^{u+1}b^{v(1+p^{m-2})+1+p^{m-2}} \end{pmatrix}$$

Since $(v + 1)(1 + p^{m-2}) = v(1 + p^{m-2}) + 1 + p^{m-2}$, $\beta\alpha = \alpha\beta^{1+p^{m-2}}$ or $\alpha^{-1}\beta\alpha = \beta^{1+p^{m-2}}$ and G is unique.

THEOREM 11: If $m > 3$, there are four and only four non-Abelian groups of order 2^m each containing an element of order 2^{m-1}.

Proof: Let b be an element of order 2^{m-1} in a non-Abelian group G of order 2^m if such a group exists where m is greater than 3. Suppose the only element of order 2 is the single element of order 2 in $\{b\}$, that being the element $b^{2^{m-2}}$. Since G is non-Abelian it is non-cyclic by Corollary 2 of Theorem a. The group G satisfies the hypothesis of Theorem 9 and since it is non-cyclic it is the last type defined in Theorem 9 and was shown to be unique.

It remains to consider when G contains an element a of order 2 not contained in $\{b\}$. By Theorem 4, $\{b\}$ is normal in G and hence there is an integer i such that $a^{-1}ba = b^i$ where $1 < i < 2^{m-1}$. By Lemma 3, $a^{-2}ba^2 = b^{i^2}$. However a is of order 2 and hence $b = b^{i^2}$. Since b is of order 2^{m-1}, $i^2 \equiv 1 \bmod 2^{m-1}$. Now i is an odd integer for if it were not, $a^{-1}ba = b^{2n}$ for some positive integer n. Raising both sides of the last equation to the power 2^{m-2} yields $a^{-1}b^{2^{m-2}}a = b^{2^{m-1}n} = e$ which implies that $b^{2^{m-2}} = e$ which is not true. Thus $i = 1 + 2^s k$ for some positive integer s and some positive odd integer k. Now $s < m - 1$ for otherwise $a^{-1}ba = b^{1+2^s k}$ would imply that a and b are

permutable which is contrary to the hypothesis that G is non-Abelian. Now $i^2 - 1 \equiv 0 \bmod 2^{m-1}$. Hence

$$i^2 - 1 = (1 + 2^s k)^2 - 1 = 2^{s+1}k = 2^{2s}k^2 = 2^{s+1}(k + 2^{s-1}k^2) \equiv 0 \bmod 2^{m-1}.$$

Since k is odd and $s < m - 1$ either $s = m - 2$, or $s = 1$ and $2^2(k + k^2) \equiv 0 \bmod 2^{m-1}$. In the first case $i = 1 + 2^{m-2}k$. Thus $1 + 2^{m-2}k < 2^{m-1}$ which implies that $1 < 2^{m-2}(2 - k)$. Hence since k is an odd positive integer, $k = 1$ and $i = 1 + 2^{m-2}$. In the second case, $k(1 + k) \equiv 0 \bmod 2^{m-3}$, but since k is odd it follows that $1 + k \equiv 0 \bmod 2^{m-3}$. Thus $k = -1 + 2^{m-3}t$ where t is an integer and $i = -1 + 2^{m-2}t$. Now t is positive for if it were not k would be negative which is not true. Now $i < 2^{m-1}$ implies that $-1 + 2^{m-2}t < 2^{m-1}$ which in turn implies that $-1 < 2^{m-2}(2 - t)$. The only possible values for t are $t = 1$ and $t = 2$. Thus this second case gives rise to two subcases those being $i = -1 + 2^{m-2}$ and $i = -1 + 2^{m-1}$. In all three cases note that $b^{2^{m-1}} = a^2 = e$. In the case where $i = 1 + 2^{m-2}$, $aba = b^{1+2^{m-2}}$ since $a^{-1} = a$. In the case where $i = -1 + 2^{m-2}$, $aba = b^{-1+2^{m-2}}$ or $(ab)^2 = b^{2^{m-2}}$. When $i = -1 + 2^{m-1}$, $aba = b^{-1+2^{m-1}}$ or $(ab)^2 = e$. In each case the elements of G are $b^u a^v$ where $u = 0, 1, 2, \ldots, 2^{m-1} - 1$ and $v = 0, 1$. It now remains to show that in each of the three cases G exists and is unique.

When $aba = b^{1+2^{m-2}}$, multiplying $b^u a^v$ on the left by b yields the permutation

$$\varphi = \begin{pmatrix} b^u a^v \\ b^{u+1} a^v \end{pmatrix}.$$

Multiplying on the left by a yields

$$ab^{u}a^{v} = b^{1+2^{m-2}}ab^{u-1}a^{v} = b^{2+2(2^{m-2})}ab^{u-2}a^{v} = \ldots = b^{u(1+2^{m-2})}a^{v+1}.$$

This determines the permutation

$$\alpha = \begin{pmatrix} b^{u}a^{v} \\ b^{u(1+2^{m-2})}a^{v+1} \end{pmatrix}.$$

It is obvious that

$$\beta^{2^{m-1}} = \alpha^{2} = \begin{pmatrix} b^{u}a^{v} \\ b^{u}a^{v} \end{pmatrix}$$

Which is the identity permutation. Now

$$\alpha\beta\alpha = \begin{pmatrix} b^{u}a^{v} \\ b^{u(1+2^{m-2})}a^{v+1} \end{pmatrix}\begin{pmatrix} b^{u}a^{v} \\ b^{u+1}a^{v} \end{pmatrix}\begin{pmatrix} b^{u}a^{v} \\ b^{u(1+2^{m-2})}a^{v+1} \end{pmatrix} = \begin{pmatrix} b^{u}a^{v} \\ b^{u+1+2^{m-2}}a^{v} \end{pmatrix} = \beta^{1+2^{m-2}}.$$

and hence in the first case G exists and is unique.

When $(ab)^{2} = b^{2^{m-2}}$, multiplying $b^{u}a^{v}$ on the left by b yields the permutation

$$\beta = \begin{pmatrix} b^{u}a^{v} \\ b^{u+1}a^{v} \end{pmatrix}.$$

Now

$$a(b^{u}a^{v}) = (ab)b^{u+1}a^{v} = (b^{-1+2^{m-2}}a)b^{u-1}a^{v} = \ldots = b^{u(2^{m-2}-1)}a^{v+1}.$$

This determines the permutation

$$\alpha = \begin{pmatrix} b^{u}a^{v} \\ b^{(2^{m-2}-1)}a^{v+1} \end{pmatrix}.$$

It is obvious that

$$\beta^{2^{m-1}} = \alpha^2 = \begin{pmatrix} b^u a^v \\ b^u a^v \end{pmatrix}.$$

Now

$$(\alpha\beta)^2 = \left[\begin{pmatrix} b^u a^v \\ b^{u(2^{m-2}-1)} a^{v+1} \end{pmatrix}\begin{pmatrix} b^u a^v \\ b^{u+1} a^v \end{pmatrix}\right]^2 = \begin{pmatrix} b^u a^v \\ b^{u(2^{m-2}-1)+1} a^{v+1} \end{pmatrix}^2 = \begin{pmatrix} b^u a^v \\ b^{u+2^{m-2}} a^v \end{pmatrix} = 2^{m-2}$$

and hence in the second case G exists and is unique.

When $(ab)^2 = e$, multiplying $b^u a^v$ on the left by b determines the permutation

$$\beta = \begin{pmatrix} b^u a^v \\ b^{u+1} a^v \end{pmatrix}.$$

Now

$$a(b^u a^v) = abb^{u-1} a^v = b^{-1} ab^{u-1} a^v = \ldots = b^{-u} a^{v+1}.$$

This determines the permutation

$$\alpha = \begin{pmatrix} b^u a^v \\ b^{-u} a^{v+1} \end{pmatrix}.$$

It is obvious that

$$\beta^{2^{m-1}} = \alpha^2 = \begin{pmatrix} b^u a^v \\ b^u a^v \end{pmatrix}.$$

Now

$$(\alpha\beta)^2 = \left[\begin{pmatrix} b^u a^v \\ b^{-u} a^{v+1} \end{pmatrix}\begin{pmatrix} b^u a^v \\ b^{u+1} a^v \end{pmatrix}\right]^2 = \begin{pmatrix} b^u a^v \\ b^{1-u} a^{v+1} \end{pmatrix}^2 = \begin{pmatrix} b^u a^v \\ b^u a^v \end{pmatrix}.$$

Hence in the third case G exists and is unique. This proves the theorem.

ACKNOWLEDGEMENT

The author wishes to express his sincere appreciation to Dr. Richard L. Yates for his patient assistance in the preparation of this report.

REFERENCES

Burnside, W. Theory of Groups of Finite Order. Cambridge: University Press, 1897.

Carmichael, Robert D. Introduction to the Theory of Groups of Finite Order. New York: Dover Publications, 1956.

Fuchs, L. Abelian Groups. Oxford: Pergamon Press, 1960.

Hall, Marshall, Jr. The Theory of Groups. New York: The Macmillan Company, 1959.

Hilton, Harold. An Introduction to the Theory of Groups of Finite Order. Oxford: Clarendon Press, 1908.

Kurosh, A. G. The Theory of Groups. New York: Chelsea Publishing Company, 1956.

Ledermann, Walter. Introduction to the Theory of Finite Groups. New York: Interscience Publishers, 1957.

Specht, Wilhelm. Gruppentheorie. Berlin: Springer-Verlag, 1956.

Zassenhaus, Hans J. The Theory of Groups. New York: Chelsea Publishing Company, 1958.

PRIME-POWER GROUPS

by

GERALD CLARK SCHRAG

A. B., Bethel College, 1960

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1964

Any finite group may be generated by a certain set of prime-power groups. It is because of this that the theory of prime-power groups is very important in the application of finite group theory. Thus many theorems which can be proven about prime-power groups may be used to prove other theorems concerning finite group theory in general.

It is the purpose of this report to present in a logical order some of the basic properties of prime-power groups. The first section is concerned with presenting some simple properties which are common to all prime-power groups. These properties have to do with self-conjugate elements and normal subgroups of any prime-power group.

It is often interesting and helpful to know how many subgroups of a given order are contained in a given prime-power group. If not enough information is given about the subgroups it still may be possible to obtain some information about the original group. This original group is shown to be cyclic if it is of an odd order and either cyclic or of only one other possible type if it is of even order.

It is shown in the last section that if a non-Abelian prime-power group contains an element of highest possible order such that it is not a generator of the group, there is one and only one such group if it is of odd order and exactly four such groups of even order provided the order of the group is large enough.