ABSTRACT GROUPS OF CERTAIN ORDERS

by

AUGUST W. WALTMANN

B. A., Wartburg College, 1964

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF ARTS

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas
1966

Approved By:

Richard Yates
Major Professor

TABLE OF CONTENTS

INTRODUCTION

The discovery of all abstract groups of a preassigned order has been of interest to algebraists since the conception of group theory. No successful method has yet been discovered for constructing all possible abstract groups of a preassigned order, nor do we know in advance how many such groups exist, except in a few relatively simple cases. This report contains four of these elementary cases. Cases considered are abstract groups of order p, p^2, pq, and p^3 where p and q are primes.

A basic understanding of the properties of integers and elementary group theory will be assumed on the part of the reader.

In the initial pages of this report definitions, theorems, and a corollary are stated that will be used in proving theorems of major interest in the body of the report.

Throughout the paper "e" will be used to represent the unit element; the "identity". The notation and nomenclature of multiplication will be adopted to express the composition of abstract group elements. Groups and subgroups will be denoted by capital letters G, H, K, ..., while the elements will be denoted by lower case letters a, b, c, ... Thus for any two elements a and b, equal or unequal, belonging to a group G there exists a unique element c belonging to G such that ab = c.

The symbol (a, b) = d will be used to mean that d is the greatest common divisor of a and b where a, b, d are integers. In the special case

when d = 1 we say that a and b are relatively prime. The symbol $\cap$ will be used to indicate the usual set intersection but $\cup$ will not denote ordinary set union. Let H and K be subgroups of a group G. Then the symbol H $\cup$ K will represent that subgroup of G, called the union of H and K, consisting of the set of all finite products, $g_1 g_2 \cdots g_s$, where each g_i belongs to H or K.

On the following pages will be found a list of definitions, theorems and a corollary which will be used throughout the paper.

DEFINITION A: If a is an element of a group G, then the least positive integer h for which $a^h = e$ is called the order of the element a. If no such h exists, a is said to have zero order.

DEFINITION B: The order of a group G is the cardinal number of elements in G.

DEFINITION C: A group whose elements can all be expressed as powers of a single element is called a cyclic group. In general a cyclic group C of order c consists of the c elements e, a, a^2, $\cdots$, a^{c-1} where c is the least positive integer such that $a^c = e$. We say that C is generated by a and write C = [a].

DEFINITION D: An abstract group is an equivalence class of all groups isomorphic to a given group.

THEOREM A: There is one and only one (abstract) cyclic group for any given order.

DEFINITION E: A subset H of elements of a group G is called a

subgroup of G if it forms a group with respect to the product as defined in G. A subgroup H of G is called a proper subgroup of G if H is not G itself and if H has at least one element other than the unit element.

THEOREM B: (Lagrange). If H is a subgroup of G where the orders of these groups are h and g respectively, then h is a factor of g, g = nh for n a positive integer.

COROLLARY B-1: If G is a group of order g, the order of every element of G is a factor of g.

THEOREM C: (Fermat). If p is a prime then $n^p \equiv n \pmod{p}$.

DEFINITION F: Given any two abstract groups A and B of orders g and h respectively, we may form from these the set of ordered pairs (a, b), $a \in A$, $b \in B$. These ordered pairs will be the elements of a new group of order gh called the direct product of A and B, denoted $A \times B$, if we define product by the rule $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

THEOREM D: If $G = A \times B$ then G contains subgroups A* and B* isomorphic to A and B respectively such that every element of A* commutes with every element of B*.

THEOREM E: The direct product of Abelian groups is Abelian.

THEOREM F: If A and B are subgroups of a group G such that,
i) ab = ba for every element $a \in A$ and every element $b \in B$, and
ii) $A \cap B = e$, then $A \times B$ is isomorphic to a subgroup of G.

DEFINITION G: A subgroup H of a group G is said to be a normal subgroup of G if $x^{-1} Hx = H$ for all $x \in G$.

THEOREM G: A group G is isomorphic to the direct product of two subgroups A and B if A and B are normal subgroups such that $A \cap B = e$, $A \cup B = G$.

THEOREM H: If m and n are relatively prime, then a cyclic group of order mn is isomorphic to the direct product of cyclic groups of orders m and n; $[mn] \approx [m] \times [n]$.

DEFINITION H: The aggregate of those elements of a group G which commute with all elements of G is called the center Z of G.

THEOREM I: The center Z of a group G is a normal subgroup of G.

DEFINITION I: The kernel of a homomorphism of a group G onto a group H is that subset T of G that is mapped onto the identity element of H.

THEOREM J: The kernel T of a homomorphism of a group G is a normal subgroup of G.

DEFINITION J: Given a group G and a subgroup H, the set of elements hx, $h \in H$, $x \in G$, x fixed, is called a right coset of H. We write Hx to designate this set. Similarly, the set of elements xh, $h \in H$ is called a left coset xH of H.

THEOREM K: Two left (right) cosets of H in G are either disjoint or identical sets of elements.

THEOREM L: A left (right) coset of H contains the same cardinal number of elements as H.

DEFINITION K: The cardinal number r of left (right) cosets of a subgroup H in a group G is called the index of H in G.

DEFINITION L: If the index of a subgroup H in a group G is r, we will

write $G = H + Hx_2 + \cdots + Hx_r$, to indicate that the cosets H, Hx_2, $\cdots$, Hx_r are disjoint and exhaust G. Here the indicated addition is only a convenient notation and not to be regarded as an operation.

DEFINITION M: If G is a group and T is a normal subgroup, then the group H, consisting of the cosets Tx_i as elements under the product $(Tx_i)(Tx_j) = Tx_k$ if $x_i x_j \in Tx_k$ in G, is called the factor group of G with respect to T written $H = G/T$.

THEOREM M: The order of $H = G/T$ is r, the index of T in G.

THEOREM N: Given a group G and a normal subgroup T, then if $H = G/T$, there is a homomorphism $G \rightarrow H$ whose kernel is T. This homomorphism is given by $g \rightarrow Tx_i$, if $g \in Tx_i$ in G.

DEFINITION N: If p is a prime, a group G is a p-group in case every element $x \in G$ except the identity has order some power of p.

THEOREM O: (Cauchy). If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

DEFINITION O: If H is a given subgroup of G, any subgroup of the form aHa^{-1} where $a \in G$ is said to be conjugate with H relative to G.

DEFINITION P: Let H be a subgroup of G. The normalizer of H in G is the set of all $a \in G$ such that $aHa^{-1} \subset H$.

THEOREM P: The number of distinct subgroups of a group G conjugate with a given subgroup H is equal to the index of the normalizer of H in G.

DEFINITION Q: A subgroup S of a group G is a Sylow subgroup of G

if it is a p-group and is not contained in any larger p-group which is a subgroup of G.

THEOREM Q: (First Sylow Theorem). If G is of order $n = p^m s$ where p does not divide s, p a prime, then G contains subgroups of orders p^i, $i = 1, \cdots, m$, and each subgroup of order p^i, $i = 1, \cdots, m-1$, is a normal subgroup of at least one subgroup of order p^{i+1}.

THEOREM R: (Second Sylow Theorem). Let G be a finite group with p-Sylow subgroup P. All p-Sylow subgroups of G are conjugate to P, and the number of these subgroups is $\equiv 1 \pmod{p}$, and is a divisor of the order of G.

THEOREM S: Every proper subgroup of a p-group P of order p^m is contained in a maximal proper subgroup of order p^{m-1}, and all the maximal subgroups of P are normal subgroups.

THEOREM T: A finite Abelian group of order $n = p_1^{c_1} \cdots p_r^{c_r}$, the p_i being distinct primes, is the direct product of Sylow subgroups $S(p_1), \cdots, S(p_r)$. Here $S(p_i)$ is of order $p_i^{c_i}$ and is the direct product of cyclic groups of orders $p_i^{c_{i1}}, \cdots, p_i^{c_{is}}$ where $c_{i1} + \cdots + c_{is} = c_i$.

DEFINITION R: If A is an Abelian p-group which is the direct product of cyclic groups of orders $p^{c_1}, \cdots, p^{c_r}$, then these numbers are called the invariants of the group.

THEOREM U: Two finite Abelian p-groups are isomorphic if and only if they have the same invariants.

GROUPS OF ORDER p

THEOREM I: There exists exactly one group of order p for any prime p and it is necessarily cyclic.

PROOF: If G is a group of prime order p, then by the Lagrange theorem, the order of any subgroup of G must either be 1 or p. Hence the only subgroups of G are the improper subgroups; a subgroup of G is either just the unit element e or all p of the elements of G.

If a is an element of G other than e, its order, being greater than 1 must be p since the order of elements of G must divide the order of G by Corollary B-1. Hence e, a, $a^2, \ldots, a^{p-1}$ ($a^p = e$) are the p elements of G. Thus G is cyclic. Since G must be cyclic, there exists exactly one abstract group of order p for any prime by Theorem A.

GROUPS OF ORDER p^2

THEOREM II: A group of order p^2 where p is a prime is Abelian and is either cyclic or isomorphic to the direct product of two distinct cyclic subgroups of order p whose intersection is the identity of the group.

PROOF: Let G be a group of order p^2. Then, according to the First Sylow Theorem, G contains subgroups of orders p and p^2 and each subgroup

of order p is a normal subgroup of the subgroup of order p^2. Since the subgroup of order p^2 is G, G can be the cyclic group of order p^2. Let a be an element of G of order p^2. Then G consists of the p^2 elements e, a, a^2, ..., a^{p^2-1} ($a^{p^2} = e$).

If G is not the cyclic group of order p^2, then G contains no element of order p^2. Since G is a p-group, the elements of G must have order p or 1. Obviously not all elements of G can be of order 1 since G is of order p^2. Hence elements of G other than the identity e must be of order p. Since G is of order p^2, G will contain two distinct cyclic subgroups of order p, say $[b]$ and $[c]$, where $b^p = e$, $c^p = e$ and $[b] \cap [c] = e$. According to Theorem S $[b]$ and $[c]$ are maximal subgroups and both subgroups are normal subgroups of G. Hence, by Theorem G, $G \approx [b] \times [c]$. Since it is true that G is the direct product of the subgroups $[b]$ and $[c]$, all elements of G commute with all other elements of G. Hence in this case, also, G is Abelian.

GROUPS OF ORDER pq

THEOREM III: A group of order pq, where $p > q$ are primes, is either cyclic or a non-Abelian group generated by two elements a and b satisfying the following relations:

$$b^p = e;\ a^q = e;\ a^{-1}ba = b^r$$

where $r \not\equiv 1 \pmod p$ but $r^q \equiv 1 \pmod p$. The second possibility occurs if and

only if q divides p - 1.

PROOF: Let G be a group of order pq where $p > q$ are primes. According to the theorem of Cauchy, since G is a finite group, G contains an element of order p. Let b be an element of order p in G. Then b generates a cyclic subgroup $S = [b]$ of G. S consists of the p elements $e, b, b^2, \ldots, b^{p-1}$ ($b^p = e$). Since the highest power of p that divides pq is one, S is a p-Sylow subgroup of G. The number of p-Sylow subgroups of G conjugate to S, according to the Second Sylow Theorem, is congruent to 1(mod p) and is also a divisor of pq. Hence the number of conjugates to S is $1+vp$ for some integer $v \geq 0$. Since $1+vp$ and p are relatively prime and $1+vp$ divides pq, $1+vp$ must divide q. Hence $v = 0$ since $p > q$. Thus the index of the normalizer of S in G is one by Theorem P. Therefore $aSa^{-1} \subseteq S$ for every $a \in G$ so that S is a normal subgroup of G.

According to the Cauchy theorem G also contains an element of order q. Let this element be a. Thus a generates a cyclic subgroup $T = [a]$ of G. T consists of the q elements $e, a, a^2, \ldots, a^{q-1}$ ($a^q = e$). The highest power of q that divides pq is one, hence T is a q-Sylow subgroup of G. The number of q-Sylow subgroups of G conjugate to T is $1+kq$ for some integer $k \geq 0$ since, according to the Second Sylow Theorem the number is congruent to 1(mod q). The number of conjugates of T divides pq. Since $1+kq$ and q are relatively prime and $1+kq$ divides pq, $1+kq$ must divide p. Two possibilities thus result. Either $k = 0$ or $p - 1$ is divisible by q.

Case 1: If $k = 0$ the index of the normalizer of T in G is one by Theorem

P. Hence $aTa^{-1} \subseteq T$ for every element $a \in G$. Thus in this case T and S are both normal subgroups of G. Hence for every prime p that divides the order of G, every p-Sylow subgroup is normal. Since S and T are of prime orders p and q respectively, where $p > q$, $S \cap T = e$. The elements of the subgroup $S \cup T$ are all the finite products of elements of S with elements of T. However, all these finite products are equivalent to products of two elements, one from S and one from T, since both S and T are cyclic normal subgroups of G. Also, $a^i b^j = a^k b^h$ implies $i = k$ and $j = h$. Thus the subgroup $S \cup T$ has pq elements so that $S \cup T = G$. Therefore, according to Theorem G, $G \approx S \times T$, G is isomorphic to the direct product of the two cyclic subgroups S and T of orders p and q respectively. Since $p > q$ are primes they are relatively prime. Hence by Theorem H, $S \times T$ is isomorphic to the cyclic group of order pq. Thus for this case G is a cyclic group of order pq.

Case 2: If $p - 1$ is divisible by q, then T could still be normal. If T is normal, G is a cyclic group of order pq as discovered above.

Assume T is not a normal subgroup of G. Since S is a normal subgroup of G, S commutes with every element of G. Hence $ba = ab^r$ for some integer r less than p. If $r = 1$, then all elements of S commute with all elements of T (elements of T commute with elements of T since T is cyclic). Thus for $r = 1$, T would be a normal subgroup of G and G would be the cyclic group of order pq found in Case 1 above. Hence $r \neq 1$ and G is non-Abelian.

Since $r \neq 1$, $ba = ab^r$ implies $a^{-1}ba = b^r$. Consider $a^{-1}b^i a$

$= a^{-1}bbb\cdots ba = (a^{-1}ba)(a^{-1}ba)\cdots(a^{-1}ba) = b^r b^r \cdots b^r = b^{ir}$. Hence

(1) $\quad a^{-1}b^i a = b^{ir}$ for any integer i.

In particular

(2) $\quad a^{-1}b^r a = b^{rr} = b^{r^2}$.

Upon substituting $a^{-1}ba$ for b^r in equation (2) the equation becomes $a^{-2}ba = b^{r^2}$. A similar statement is needed for all powers of r. Consider the proposition

(3) $\quad P(n)$: $a^{-n}b^i a^n = b^{ir^n}$ for all positive integers n and any integer i.

Then P(1) is $a^{-1}b^i a = b^{ir^1}$ which was proved above, equation (1). Assume P(k) is true:

(4) $\quad a^{-k}b^i a^k = b^{ir^k}$.

Then multiplying on the left by a^{-1} and on the right by a on each side of equation (4) the following equations are obtained: $a^{-1}a^{-k}b^i a^k a$ $= a^{-k-1}b^i a^{k+1} = a^{-1}b^{ir^k}a$. Since $a^{-1}b^i a = b^{ir}$ for any integer i, $a^{-1}b^{ir^k}a = b^{ir^k r} = b^{ir^{k+1}}$. Hence $a^{-k-1}b^i a^{k+1} = b^{ir^{k+1}}$ so that P(k+1) holds. Therefore P(n) is true for all positive integers n and any integer i.

In particular let n = q and i = 1. Then $a^{-q}ba^q = b^{r^q}$. Since $a \in T$ is

of order q, $a^{-q}ba^{q} = b$. Hence $b^{r^{q}} = b$ from which it follows that $r^{q} \equiv 1 \pmod{p}$ if G is a group satisfying the conditions of the second half of the theorem.

Sufficiency of the condition $r^{q} \equiv 1 \pmod{p}$, and $r \not\equiv 1 \pmod{p}$ is now to be proved. Assume G is a group defined by elements a and b satisfying relations: $b^{p} = e$; $a^{q} = e$; $a^{-1}ba = b^{r}$ where $r \not\equiv 1 \pmod{p}$ but $r^{q} \equiv 1 \pmod{p}$. It will be shown that these conditions are sufficient to prove that G has order pq.

It was shown in equation (1) above that $a^{-n}b^{i}a^{n} = b^{ir^{n}}$ for all integers n and any integer i. Let u, v, x, and y represent integers. Then in particular, $a^{-x}b^{v}a^{x} = b^{vr^{x}}$. Thus $(a^{u}b^{v})(a^{x}b^{y}) = a^{u}a^{x}a^{-x}b^{v}a^{x}b^{y}$ $= a^{u+x}(a^{-x}b^{v}a^{x})b^{y} = a^{u+x}b^{vr^{x}+y}$. Hence

$$(a^{u}b^{v})(a^{x}b^{y}) = a^{u+x}b^{vr^{x}+y} \tag{5}$$

is a general rule for multiplying any two elements of G. Consider the proposition

$$P(n):\ (a^{u}b^{v})^{n} = a^{nu}b^{v(r^{(n-1)u}+r^{(n-2)u}+\cdots+1)} \text{ for all positive integers n, any integers u and v, and for the particular positive integer r.} \tag{6}$$

Letting n = 1, P(1) becomes $(a^{u}b^{v})^{1} = a^{u}b^{v(r^{0})} = a^{u}b^{v}$. Assume P(n) is true for n = k:

(7) $(a^u b^v)^k = a^{ku} b^{v(r^{(k-1)u} + r^{(k-2)u} + \cdots + 1)}$.

Multiplying on both sides of equation (7) by $(a^u b^v)$ yields the equations:

$(a^u b^v)^k (a^u b^v) = (a^u b^v)^{k+1} = a^{ku} b^{v(r^{(k-1)u} + r^{(k-2)u} + \cdots + 1)} (a^u b^v)$

$= a^{ku+u} b^{v(r^{(k-1)u} + r^{(k-2)u} + \cdots + 1) r^u + v}$

$= a^{(k+1)u} b^{v(r^{ku} + r^{(k-1)u} + \cdots + 1)}$. Thus it follows from these equations that $(a^u b^v)^{k+1} = a^{(k+1)u} b^{v(r^{ku} + r^{(k-1)u} + \cdots + 1)}$ which is P(k+1). Therefore P(n) is true for all positive integers n.

In particular $(a^u b^v)^{pq} = a^{pqu} b^{v(r^{(pq-1)u} + r^{(pq-2)u} + \cdots + 1)}$. Note that $r^{(pq-1)u} + r^{(pq-2)u} + \cdots + 1$ is just a geometric progression with common ratio r^{-u}. The sum of the first pq terms is $\left(\frac{r^{(pq-1)u} - r^{-u}}{1 - r^{-u}}\right)$

$= \left(\frac{r^{pqu} - 1}{r^u - 1}\right)$. Hence $(a^u b^v)^{pq} = a^{pqu} b^{v\left(\frac{r^{pqu} - 1}{r^u - 1}\right)} = (a^q)^{pu} b^{v\left(\frac{r^{pqu} - 1}{r^u - 1}\right)}$

$= b^{v\left(\frac{r^{pqu} - 1}{r^u - 1}\right)}$. Thus what must be shown is that p divides $\left(\frac{r^{pqu} - 1}{r^u - 1}\right)$.

If $(p, r^u - 1) \neq 1$, then $(p, r^u - 1) = p$ since p is a prime. Hence p divides $r^u - 1$. Thus $r^u \equiv 1 \pmod{p}$. Since q is a prime satisfying $q > u \geq 1$, $(u, q) = 1$. Thus there exist integers s and t such that $1 = us + qt$. Since $r^u \equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$, $r = r^{us+qt}$

$= (r^u)^s (r^q)^t \equiv 1 \pmod{p}$. However $r \equiv 1 \pmod{p}$ contradicts the original

condition on r. Hence $(p, r^u - 1) = 1$.

Let $M = r^{(pq-1)u} + r^{(pq-2)u} + \cdots + r^u + 1 = \left(\frac{r^{pqu} - 1}{r^u - 1}\right)$. $M = \left(\frac{r^{pqu} - 1}{r^u - 1}\right)$ is obviously an integer since the integers are closed under multiplication and addition. Since $r^{pqu} = (r^q)^{pu} \equiv 1 \pmod{p}$, p divides $r^{pqu} - 1$. Hence p divides $\left(\frac{r^{pqu} - 1}{r^u - 1}\right)$ as was desired to be proved. Thus $M = hp$ for some integer h and $b^{v\left(\frac{r^{pqu} - 1}{r^u - 1}\right)} = b^{vhp} = (b^p)^{vh} = e$. Therefore for all integers u and v, $(a^u b^v)^{pq} = a^{pqu} b^{vhp} = e$. Hence the order of G is a divisor of pq.

Since $p > q$ are primes, the only divisors of pq are 1, p, q, and pq. G is not of order 1 since G is generated by two elements by assumption. Since a is of order q, $(ea)^p = a^p \neq e$. Hence G is not of order p. Similarly $(eb)^q = b^q \neq e$ since b is of order p. Hence G is not of order q either. Thus the order of G must be pq. Also, since $ba = ab^r \neq ab$, G is non-Abelian and hence non-cyclic. G is thus a non-Abelian group of order pq defined by two elements a and b satisfying the relations $b^p = e$; $a^q = e$; $a^{-1}ba = b^r$ if and only if $r \not\equiv 1 \pmod{p}$ but $r^q \equiv 1 \pmod{p}$. Thus two distinct groups of order pq have been found.

As an example of when Theorem III may be applied, consider the groups of order 6. According to this theorem, an abstract cyclic group of order 6 does exist. Since $6 = 2 \cdot 3$, let $p = 3$ and $q = 2$. Then since 2 divides $3 - 1$, an abstract non-Abelian group of order 6 exists with defining relations

$b^3 = e$, $a^2 = e$, and $a^{-1}ba = b^2$. Thus two abstract groups of order 6 exist and these are the only abstract groups of order 6.

Consider the groups of order 15. They serve as a contrasting example of what this theorem purports. Again an abstract cyclic group of order 15 exists. However since $15 = 3 \cdot 5$, letting $p = 5$, and $q = 3$, we see that 3 does not divide 5 - 1. Hence, only one abstract group of order 15 exists.

GROUPS OF ORDER p^3

THEOREM IV: A group of order p^3 where p is a prime must be one of the following five types:

A) Abelian

1) $a^{p^3} = e$

2) $a^{p^2} = e$, $b^p = e$, $ba = ab$

3) $a^p = b^p = c^p = e$, $ba = ab$, $ca = ac$, $cb = bc$

B) Non-Abelian of order $2^3 = 8$

4) Dihedral: $a^4 = e$, $b^2 = e$, $ba = a^{-1}b$

5) Quaternion: $a^4 = e$, $b^2 = a^2$, $ba = a^{-1}b$

C) Non-Abelian of order p^3, p odd

4) $a^{p^2} = e$, $b^p = e$, $b^{-1}ab = a^{1+p}$

5) $a^p = b^p = c^p = e$, $ab = bac$, $ca = ac$, $cb = bc$.

PROOF: Let G be a group of order p^3 where p is a prime. Clearly the set of invariants for G is (p^3), (p^2, p), or (p, p, p). Hence by Theorem T, G might be one of the three Abelian types with invariants respectively (p^3), (p^2, p), and (p, p, p). Theorem U requires that the groups with these sets of invariants are distinct Abelian groups (not isomorphic). Thus G might be one of the three Abelian types listed under A) of the theorem. Since exactly three sets of invariants exist for p^3, by Theorem U exactly three types exist of order p^3. Tables I, II, and III on pages 27 and 28 give these distinct Abelian groups for p = 2.

The discussion of non-Abelian groups of order p^3 naturally divides into two cases, one when p is the even prime, 2, and the other when p is an odd prime.

Case 1: Let H be a non-Abelian group of order $2^3 = 8$. Factors of 8 are 1, 2, 4, and 8. Hence by Corollary 1 of Theorem B, all the elements of H are of order 1, 2, 4, or 8. No element of H can be of order 8 since if such an element did exist, H would be the cyclic group of order 8 and thus Abelian. Obviously not all the elements of H are of order 1. If all the elements of H are of order 2, then for $a \in H$ and $b \in H$, $a^2 = e$, $b^2 = e$, and $(ab)^2 = e$ or equivalently

(1) $\qquad abab = e.$

Thus if both sides of equation (1) are multiplied on the left by a and on the right be b the result is $a^2bab^2 = ab$. Since $a^2 = e$ and $b^2 = e$, it is also true

that $a^2bab^2 = ebae = ba$. Thus the assumption that all elements of H are of order 2 leads to the conclusion that $ab = a^2bab^2 = ba$. This is a contradiction of the fact that H is non-Abelian. Hence, not all the elements of H are of order 2; H must contain an element of order 4, say $a^4 = e$.

If $b \in H$ but $b \notin [a] = A$, then the eight elements of H are e, a, a^2, a^3, b, ab, a^2b, a^3b. The closure property of a group demands that $b^2 \in H$; hence $b^2 \in A$ since a and b are independent. If $b^2 = a$ or $b^2 = a^3$, then b would be of order 8. Hence $b^2 = e$ or $b^2 = a^2$. According to Theorem S, A is a normal subgroup of H. Hence $b^{-1}ab \in A$. If we assume that $b^{-1}ab = e$ then we must conclude that $a = e$, hence $b^{-1}ab \neq e$. If $b^{-1}ab = a$, then H would be Abelian. Hence $b^{-1}ab \neq a$. Similarly if $b^{-1}ab = a^2$, then $b^{-1}ab$ is of order 2. Thus $(b^{-1}ab)^2 = e$. However, $(b^{-1}ab)^2 = b^{-1}abb^{-1}ab = b^{-1}a^2b$. Hence it follows that $b^{-1}a^2b = e$ or equivalently $a^2b = b$. Thus the assumption that $b^{-1}ab = a^2$ leads to the false conclusion that $a^2bb^{-1} = bb^{-1} = e$; a is of order 4, not 2. Therefore it must be true that $b^{-1}ab = a^3$.

Thus it follows that exactly two non-Abelian groups of order 8 exist. One of these groups is called the dihedral group and has defining relations $a^4 = e$, $b^2 = e$, and $b^{-1}ab = a^3$. The other is called the quaternion group and has defining relations $a^4 = e$, $b^2 = a^2$, and $b^{-1}ab = a^3$. Tables IV and

V on pages 28 and 29 give the respective multiplication properties of these groups. It is clear from the tables that these two groups are distinct. Note that the inverse of b for the dihedral group is b, while for the quaternion group, the inverse of b is a^2b. Similar comparisons can be made for the elements ab, a^2b, and a^3b.

Case 2: Finally, let K be a non-Abelian group of order p^3 where p is an odd prime. The elements of K will have order 1, p, p^2, or p^3 according to Corollary 1 of Theorem B, since these are the only factors of p^3. No element can be of order p^3 since non-Abelian groups are now being considered.

Suppose K has an element a of order p^2. Then $a^{p^2} = e$ and a generates a cyclic subgroup $[a] = A$ of K having p^2 elements. According to the Theorem S, A is a maximal and normal subgroup of K.

Let b be an element of K not in A, $b \notin A$. Then $b \neq e$ since $e \in A$. Hence b is not of order 1. It is also true that b is not of order p^3 since K is non-Abelian.

According to Theorem K, two left cosets of A in K are either disjoint or identical sets of elements and all cosets of A contain the same number of elements as A. Assume two left cosets of A are identical; assume $Ab^i = Ab^j$ for i and j integers such that $0 \leq i < j \leq p-1$. Then since both cosets have the same number of elements, each element in Ab^i must be

equal to an element in Ab^j. Hence, in particular,

(2) $\qquad ab^j = a^k b^i$ for some integer k, $1 < k \leq p^2$.

Multiplying on the left by a^{-1} and on the right by b^{-1} on each side of equation (2) yields $b^{j-1} = a^{k-1}$. Then $b^{j-i} \in A$. Since $0 \leq i < j \leq p-1$, it follows by manipulation of the inequality that $0 < j - i < p$. Thus $(j - i, p^2) = 1$ and $t(j - i) = 1 + sp^2$ for some integers t and s. Then $(b^{j-i})^t = b^{t(j-i)} = b^{1+sp^2} = b(b^{p^2})^s = be = b$ since b must be of order p or p^2. Hence

(3) $\qquad (b^{j-i})^t = b.$

If $b^{j-i} \in A$, then also $(b^{j-i})^t \in A$ since A is a subgroup. Thus by equation (3), $b \in A$ but this contradicts the original choice of b. Therefore cosets of A of the form Ab^i, where $0 \leq i \leq p-1$, are disjoint if the powers of b are not identical.

Since K must contain p^3 elements, it must be true that

(4) $\qquad K = A + Ab + Ab^2 + \cdots + Ab^{p-1}.$

Each of these p cosets of K obviously has p^2 elements since A has p^2 elements. This representation does exhaust K since p^3 elements are represented symbolically. Thus it must be true that $Ab^p = Ab^j$ for j integer such that $0 \leq j \leq p-1$. In particular

(5) $\qquad ab^p = a^k b^j$ for k an integer such that $1 \leq k \leq p^2$.

Multiplying on both sides of equation (5) by a^{-1} on the left and b^{-j} on the right yields $b^{p-j} = a^{k-1}$; $b^{p-j} \in A$. Since $0 \leq j \leq p-1$, $0 \leq j < p$ and $0 < p-j \leq p$. If $p-j < p$, then $(p-j, p^2) = 1$ and $u(p-j) = 1 + vp^2$ for some integers u and v. Then $(b^{p-j})^u = b^{u(p-j)} = b^{1+vp^2} = b(b^{p^2})^v = be = b$ since b must be of order p or p^2. Thus

$$(b^{p-j})^u = b. \tag{6}$$

However if $b^{p-j} \in A$, then $(b^{p-j})^u \in A$. Hence by equation (6) if $b^{p-j} \in A$ for $p-j < p$, then $b \in A$ which contradicts our choice of b. Hence $p-j = p$; $j = 0$. Thus $b^{p-j} = b^p \in A$ and $Ab^p = A$.

Since A is a normal subgroup of K, $b^{-1}ab \in A$, hence $b^{-1}ab = a^r$. Here $1 < r < p^2$ since K is non-Abelian.

Consider the proposition

$$P(n): \quad b^{-n}ab^n = a^{r^n} \text{ for all positive integers } n. \tag{7}$$

For $n = 1$, $P(1)$: $b^{-1}ab = a^r$ is true. Assume the proposition is true for $n = k$:

$$b^{-k}ab^k = a^{r^k}. \tag{8}$$

Then by multiplying on the left by b^{-1} and on the right by b on each side of equation (8), $b^{-1}b^{-k}ab^kb = b^{-k-1}ab^{k+1} = b^{-1}a^{r^k}b$

$$= \underbrace{(b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab)}_{r^k \text{ factors}} = a^r a^r \cdots a^r = (a^r)^{r^k} = a^{rr^k} = a^{r^{k+1}}.$$

Hence P(k+1) is true. Therefore P(n) is true for all positive integers. In particular, for p

(9) $$b^{-p}ab^p = a^{r^p}.$$

Since $b^p \in A$, b^p commutes with $a \in A$. Thus $b^{-p}ab^p = b^{-p}b^p a = a$.

Thus by equation (9) $a = b^{-p}ab^p = a^{r^p}$. Therefore $r^p \equiv 1 \pmod{p^2}$ or equivalently

(10) $$r^p = 1 + kp^2 \text{ for some positive integer } k.$$

It is also true by Fermat's theorem that $r^p \equiv r \pmod{p}$ or equivalently

(11) $$r = r^p - mp \text{ for some positive integer } m.$$

Thus by equations (10) and (11) $r = r^p - mp = 1 + kp^2 - mp = 1 + (kp - m)p$; hence

(12) $$r = 1 + (kp - m)p$$

and $r \equiv 1 \pmod{p}$. Since $1 < r < p^2$, equation (12) implies that $0 < kp - m < p$. Let $s = kp - m$. Then $0 < s < p$ and $r = 1 + sp$. Thus $(s, p) = 1$;

(13) $$sx + py = 1 \text{ for some integers } x \text{ and } y.$$

Hence $sx \equiv 1 \pmod{p}$. If $x < p$, let $j = x$. If $x \geq p$, $x = Qp + R$ where $0 < R < p$ ($R \neq 0$ since $(x, p) = 1$ by equation (13)). Then $sx = sQp + sR \equiv 1 \pmod{p}$ but $sQp \equiv 0 \pmod{p}$. Hence $sR \equiv 1 \pmod{p}$. Thus if $x \geq p$ in equation (13), let $j = R$. Hence a j always exists such that $j < p$ and

$js \equiv 1 \pmod{p}$; $js - 1 = hp$ for some integer h. Then by equation (7),

$b^{-j} a b^j = a^{r^j} = a^{(1+sp)^j}$. Hence

$$a^{(1+sp)^j} = a^{\left(1 + spj + \left(\frac{j(j-1)}{2}\right)(sp)^2 + \left(\frac{j(j-1)(j-2)}{6}\right)(sp)^3 + \cdots\right)}$$

$$= a^{\left(1 + sjp + \left(\frac{j(j-1)}{2}\right)s^2p^2 + \left(\frac{j(j-1)(j-2)}{6}\right)s^3pp^2 + \cdots\right)}. \quad \text{Since } a^{p^2} = e,$$

$a^{(1+sp)^j} = a^{1+sjp}$. Since $sj = 1 + hp$, $1 + sjp = 1 + (1+hp)p = 1 + p + hp^2$.

Thus $a^{(1+sp)^j} = a^{1+sjp} = a^{1+p+hp^2} = a^{1+p}$ since $a^{p^2} = e$. Therefore

(14) $$b^{-j} a b^j = a^{1+p}.$$

Since $js - hp = 1$, j and p are relatively prime. Since $j < p$, $b^j = eb^j$ so that b^j is obviously an element of one of the right cosets Ab^i, $1 \leq i \leq p-1$, of K in equation (4). Thus $b^j \notin A$.

It is now necessary to make a notational change. Since $b^j \notin A$, we may replace b^j by b. Then equation (4) becomes

(15) $$K = A + Ab + Ab^2 + \cdots + Ab^{p-1}$$

where the respective right cosets have been reduced to simplest form and the equation has been written in an orderly fashion. Note Ab^i of equation (4) may not be the same coset as Ab^i in equation (15) even though the two equations do appear the same. Also note that equation (14) now becomes

(16) $$b^{-1} a b = a^{1+p}.$$

Keeping in mind the change in notation, we see that b^p in the new notation is equal to $(b^j)^p$ in the old notation. However, $(b^j)^p = (b^p)^j \in A$ since in the old notation $b^p \in A$; $b^p = a^k$ for an integer k such that $1 \leq k \leq p^2$. Since in the new notation $b \in K$, the order of b must be p or p^2 since K is non-Abelian and $b \neq e \in A$. Thus in either case, $e = b^{p^2} = (b^p)^p = (a^k)^p = a^{kp}$. Since elements of A are of order p^2 and $a^{kp} = e$, p^2 must divide kp. Hence k must be a multiple of p, say $k = up$. Thus since $b^p = a^k$ we may write $b^p = a^{up}$.

Since $b^{-1}ab = a^{1+p}$, $(a^{1+p})^i = (b^{-1}ab)^i = (b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab)$ $= b^{-1}abb^{-1}abb^{-1}ab\cdots b^{-1}abb^{-1}ab = b^{-1}a^ib$. Thus $(a^{1+p})^i = a^{i(1+p)}$ $= b^{-1}a^ib$. Hence, as a general rule,

$$a^ib = ba^{i(1+p)}. \tag{17}$$

Thus $(ba^{-u})^p = \underbrace{(ba^{-u})(ba^{-u})\cdots(ba^{-u})}_{\text{p factors}} = b\underbrace{(a^{-u}b)(a^{-u}b)\cdots(a^{-u}b)}_{\text{p - 1 factors}}a^{-u}$

$$= b(\underbrace{ba^{-u(1+p)}(ba^{-u(1+p)})\cdots(ba^{-u(1+p)}}_{\text{p - 1 factors}})a^{-u}$$

$$= b^2\underbrace{(a^{-u(1+p)}b)(a^{-u(1+p)}b)\cdots(a^{-u(1+p)}b)}_{\text{p - 2 factors}}a^{-u(1+p)}a^{-u}$$

$$= b^2\underbrace{(ba^{-u(1+p)^2})(ba^{-u(1+p)^2})\cdots(ba^{-u(1+p)^2})}_{\text{p - 2 factors}}a^{-u(1+p)}a^{-u} = \cdots\cdots$$

$= b^{p-1}\left(a^{-u(1+p)^{p-2}}b\right)a^{-u(1+p)^{p-2}}a^{-u(1+p)^{p-3}}\cdots a^{-u(1+p)}a^{-u}$

$= b^{p-1}\left(ba^{-u(1+p)^{p-1}}\right)a^{-u(1+p)^{p-2}}a^{-u(1+p)^{p-3}}\cdots a^{-u(1+p)}a^{-u}$

$= b^{p}a^{-u\left(1+(1+p)+(1+p)^{2}+\cdots+(1+p)^{p-1}\right)}$. Therefore

(18) $\qquad (ba^{-u})^{p} = b^{p}a^{-u\left(1+(1+p)+(1+p)^{2}+\cdots+(1+p)^{p-1}\right)}$.

Upon expanding, $1+(1+p)+(1+p)^{2}+\cdots+(1+p)^{p-1}$

$= p+p+2p+3p+\cdots+(p-1)p+p^{2}Q$ where Q is an integer. Since $a^{p^{2}} = e$,

from equation (18) $(ba^{-u})^{p} = b^{p}a^{-u\left(p+p+2p+3p+\cdots+(p-1)p\right)}$

$= b^{p}a^{-up-up\left(1+2+3+\cdots+(p-1)\right)} = b^{p}a^{-up-up\left(\frac{p(p-1)}{2}\right)}$ since

$1+2+3+\cdots+(p-1) = \left(\frac{p(p-1)}{2}\right)$. Note that $\frac{p-1}{2}$ is an integer since p is an

odd prime. Thus $b^{p}a^{-up-up\left(\frac{p(p-1)}{2}\right)} = b^{p}a^{-up}{}_{(a^{p^{2}})}{}^{\left(\frac{-u(p-1)}{2}\right)} = b^{p}a^{-up}e$

$= a^{up}a^{-up} = e$. Therefore

(19) $\qquad (ba^{-u})^{p} = e$.

Now let $b_1 = ba^{-u}$. Then $b_1^{-1}ab_1 = (ba^{-u})^{-1}a(ba^{-u}) = (a^{u}b^{-1})a(ba^{-u})$

$= a^{u}(b^{-1}ab)a^{-u} = a^{u}a^{1+p}a^{-u}$ by equation (16). Thus $b_1^{-1}ab_1 = a^{u}a^{1+p}a^{-u}$

$= a^{u}a^{-u}a^{1+p} = a^{1+p}$. Hence when K has an element of order p^{2}, K has

the defining relations $a^{p^{2}} = e$, $b_1^{p} = e$, $b_1^{-1}ab_1 = a^{1+p}$. This group is of

type C) 4) in the theorem.

For the last part of Case 2, assume K has no element of order p^2; then all elements of K other than e have order p. Assume the center Z of K is of order p^2. Since Z is a subgroup of K, Z contains no elements of order p^2. Hence by Theorem II, Z is generated by two elements s and t satisfying the relations $s^p = t^p = e$, $[s] \cap [t] = e$, and $[s] \times [t] \approx Z$. Let r be an element of K not contained in Z, $r \notin Z$. Then r generates a cyclic subgroup $[r] = R$ of K of order p. Obviously all the elements of R commute with all the elements of Z since Z is the center of K. If $r^j \in Z$ for j an integer such that $1 < j < p$, then by the closure property of Z, $(r^j)^u \in Z$ for all integers u. However since $1 < j < p$, $(j, p) = 1$. Thus there exist integers u and v such that $ju = 1 + pv$. Hence $(r^j)^u = r^{ju} = r^{1+pv} = rr^{pv} = r(r^p)^v = re = r$. Thus if $r^j \in Z$, $(r^j)^u = r \in Z$ but this contradicts our choice of r. Therefore $R \cap Z = e$. By Theorem F the direct product $R \times Z$ is isomorphic to a subgroup of K, $R \times Z \subseteq K$. By the Lagrange theorem, subgroups of K must be of order 1, p, p^2, or p^3. Since it was assumed that Z was of order p^2 and $r \in R \times Z$ but $r \notin Z$, $R \times Z$ must have order greater than p^2. Hence $R \times Z$ is of order p^3 and $K \approx R \times Z$. However, since $Z \approx [s] \times [t]$, $K \approx [r] \times [s] \times [t]$. Thus by Theorem E, if the center Z of K is of order p^2, K is Abelian. Hence Z is of order p.

Consider the factor group K/Z of Z in K. Since Z is the center of K, Z is a normal subgroup of K by Theorem I. Hence we are assured by

Theorem N that K/Z is a group and since Z is of order p, K/Z is of order p^2 by Theorem M. Since any group of order p^2 is Abelian and K has no elements of order p^2, K/Z will be, according to Theorem II, of the type $x^p = e$, $y^p = e$, $xy = yx$. By Theorem N there exists a homomorphism of $K \rightarrow K/Z$. For $a \in K$ and $b \in K$ assign the mapping $a \rightarrow x$ and $b \rightarrow y$. Then $a^p \rightarrow x^p = e$; a^p is in the kernel of the homomorphism. Since the kernel of this particular homomorphism is Z, $a^p \in Z$. Thus because elements of Z are of order p since Z is of order p, $a^p = e$. Similarly, $b^p = e$ since $b^p \rightarrow y^p = e$ implies $b^p \in Z$. Also $a^{-1}b^{-1}ab \rightarrow x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e$ since K/Z is Abelian. Thus $a^{-1}b^{-1}ab = c \in Z$. If $a^{-1}b^{-1}ab = e$, then $ab = ba$. Recall that elements of Z commute with all the elements of K. Thus since a, b, and Z generate K, if $ab = ba$ K is Abelian. Hence $c \neq e$. Since all the elements of K other than e are of order p, $c^p = e$ and $[c] = Z$. Furthermore, since $a^{-1}b^{-1}ab = c$, $ab = bac$. Obviously $ac = ca$ and $bc = cb$ since $c \in Z$. Thus if K has no elements of order p^2, K is defined by the relations $a^p = b^p = c^p = e$, $ab = bac$, $ca = ac$, and $cb = bc$. This group is of type C) 5) in the theorem.

TABLES OF GROUPS OF ORDER 8

$a^8 = e$

	e	a	a^2	a^3	a^4	a^5	a^6	a^7
e	e	a	a^2	a^3	a^4	a^5	a^6	a^7
a	a	a^2	a^3	a^4	a^5	a^6	a^7	e
a^2	a^2	a^3	a^4	a^5	a^6	a^7	e	a
a^3	a^3	a^4	a^5	a^6	a^7	e	a	a^2
a^4	a^4	a^5	a^6	a^7	e	a	a^2	a^3
a^5	a^5	a^6	a^7	e	a	a^2	a^3	a^4
a^6	a^6	a^7	e	a	a^2	a^3	a^4	a^5
a^7	a^7	e	a	a^2	a^3	a^4	a^5	a^6

Table I

$a^4 = b^2 = e$

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	e	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	e
a^2b	a^2b	a^3b	b	ab	a^2	a^3	e	a
a^3b	a^3b	b	ab	a^2b	a^3	e	a	a^2

Table II

$a^2 = b^2 = c^2 = e$

	e	a	b	c	ab	ac	bc	abc
e	e	a	b	c	ab	ac	bc	abc
a	a	e	ab	ac	b	c	abc	bc
b	b	ab	e	bc	a	abc	c	ac
c	c	ac	bc	e	abc	a	b	ab
ab	ab	b	a	abc	e	bc	ac	c
ac	ac	c	abc	a	bc	e	ab	b
bc	bc	abc	c	b	ac	ab	e	a
abc	abc	bc	ac	ab	c	b	a	e

Table III

Dihedral Group $a^4 = b^2 = e,\ b^{-1}ab = a^3$

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Table IV

Quaternion Group $a^4 = e,\ a^2 = b^2,\ b^{-1}ab = a^3$

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

Table V

ACKNOWLEDGMENT

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

BIBLIOGRAPHY

Burnside, W., Theory of Groups of Finite Order, New York: The Macmillan Company, 1897.

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

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

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

Rotmann, Joseph J., The Theory of Groups: An Introduction, Boston: Allyn and Bacon, Inc., 1965.

Scott, W. R., Group Theory, Englewood Cliffs: Prentice-Hall, Inc., 1964.

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

ABSTRACT GROUPS OF CERTAIN ORDERS

by

AUGUST W. WALTMANN

B. A., Wartburg College, 1964

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF ARTS

Department of Mathematics

KANSAS STATE UNIVERSITY

Manhattan, Kansas
1966

The discovery of all abstract groups of a preassigned order has been of interest to algebraists since the conception of group theory. No successful method has yet been discovered for constructing all possible abstract groups of a preassigned order, nor has a method been developed to know in advance how many such groups exist, except in a few relatively simple cases. In this report knowledge of four elementary cases is gathered and theorems stating the nature and number of abstract groups for these cases are formulated. Cases considered are abstract groups of orders p, p^2, pq, and p^3 where p and q are primes.

In the initial pages of the report are stated definitions, theorems, and a corollary used in proving theorems formulated about the four above mentioned cases.

Groups of order p where p is a prime are considered first. Only one abstract group of order p exists and it is cyclic.

Next groups of order p^2 where p is a prime are considered. All groups of order p^2 are Abelian and two basic types exist; one is the cyclic group of order p^2 and the other is isomorphic to the direct product of two distinct cyclic subgroups, each of order p, whose intersection is the identity element.

Groups of composite order pq where p and q are primes are considered next in the report. Two abstract groups of order pq may exist. One always exists and is the cyclic (Abelian) group of order pq. The other is

a non-Abelian group and exists if and only if the smaller prime divides one less than the larger prime.

Finally, groups of order p^3 are considered. For each prime p, there exist three abstract Abelian groups and two abstract non-Abelian groups of order p^3. Multiplication tables for the groups of order 2^3 are exhibited to emphasize the differences between the five types of groups of order p^3.