# DETERMINATION OF GROUPS OF ORDERS 1 THROUGH 26

by

RONNIE LEE YARROW

B. S., Kansas State University, 1961

A REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1963

Approved by:

Leonard E. Fuller

Major Professor

TABLE OF CONTENTS

# INTRODUCTION

The purpose of this paper is to determine and define the abstract groups of orders one through twenty-six. It begins with the definition of a group which is followed by some elementary concepts of group theory. Most important are the concepts of subgroups, conjugate elements and subgroups, Sylow's theorem, direct products, and isomorphisms. The Sylow theorem is stated but not proved because of the length of its proof.

Finally, the theory that has been developed is used to obtain the number of and the defining relations of the groups derived. In the sense of isomorphism no two of these groups are the same. The paper is summarized by a table which compares the number of groups with the order.

Since the order of a group is a positive integer, it is necessary for the reader to have an understanding of the elementary concepts of modulo systems and partitioning from number theory. Otherwise, the material contained herein is sufficient for the understanding of the contents.

## FUNDAMENTAL CONCEPTS

Consider a set of elements a, b, ..., n which may be combined by a well defined operation. If these elements satisfy the following four postulates, then they are said to form a group.

1.) For every $a$ and $b$ in the set, the product[1] ab belongs to the set.

2.) The associative law is valid. (i.e. $(ab)c = a(bc)$.)

3.) An identity element $I$ exists such that for every $a$ in the set $aI = Ia = a$.

4.) For every $a$ in the set, there exists an inverse denoted by $a^{-1}$ such that $a^{-1}a = aa^{-1} = I$.

The group is said to be Abelian if the following postulate is added.

5.) The commutative law is valid. (i.e. $ab = ba$).

Definition 1: If a subset H of elements of a group G forms a group, then this subset is called a subgroup of G. If a subgroup H is neither G itself nor the identity $I$ alone, then H is called a proper subgroup of G.

It should be noted that under the group operation, the elements satisfy the ordinary laws of exponents.

If an element $a$ of a group is raised to a positive power $n$ and if $n$ is the least positive integer for which $a^n = I$, then $n$ is said to be the order of $a$. It follows that the element $a$ has $n$ distinct powers mod n. The powers of $a$ form a set of $n$ elements, which as has been determined above,

[1] Hereafter the term product will be used to define the operation between elements whether this operation is addition, multiplication, or some other operation. This product will be designated by the juxtaposition of the elements.

are distinct. These elements certainly satisfy the closure postulate, for the product of any two of them belongs to the set. Obviously the associative postulate holds. The identity element I is in the set, for $a^n = I$. Finally, if $a^i$ is any element of the set, then $a^{n-i}$ is its inverse for $i \neq n$. Therefore the set forms a group. But the elements also commute, and the Abelian group formed by powers of a single element is called the cyclic group of order n.

Definition 2: If the number of distinct elements of a group G is n, then n is said to be the order of G.

Hereafter when the term group is referred to, it will be assumed that its order is finite.

Theorem 1: A nonempty subset S of a group G is a subgroup if:

(i) a and b are in S, then ab is in S,

(ii) a is in S, then $a^{-1}$ is in S.

Proof: From condition (i) the subset is closed. Obviously the associative law holds since the subset is from a set in which the associative law is true. It is implied by condition (ii) that every element has an inverse in the set. The two conditions taken together imply that I is in the subset, for

$$aa^{-1} = I = a^{-1}a.$$

Thus the subset forms a group, and the theorem is proved.

Let G be a group and H a subgroup of order h of G. Then the set of elements $b_1h_i$ for $i = 1, 2, \ldots, h$, where the $h_i$ belongs to H and $b_1$ belongs to G, is called a right coset of H. This coset is denoted by $b_1H$. Similarly

Similarly $Hb_1$ is called a left coset of H. It is important to note that $IH = H$ is also a right coset. If for some $i$ and $j$, $b_1h_i = b_1h_j$, then $h_i = h_j$. This is impossible since the elements of a subgroup are distinct. Therefore the elements in each right coset are distinct. Similarly the elements in each left coset are distinct.

The concept of right coset is used in the proof of Lagrange's theorem which will be referred to several times in this paper.

Theorem 2: The order of a subgroup H of a group G is a factor of the order of G.

Proof: Let H be a subgroup of order $h$ of G. Then H is a right coset. If $g$ is the order of G, and if $g = h$; then the theorem is true. If $g > h$, then G has an element not in H, call it $b_1$. Hence $b_1H$ is another right coset of H such that $b_1H$ and H are distinct. If $b_1h_i = h_j$ for some $i$ and $j$, then $b_1 = h_jh_i^{-1}$. This is contrary to the choice of $b_1$. If $g = 2h$, then the theorem is proved. If $g > 2h$, then G contains another element $b_2$ different from $b_1$ which is not in H or $b_1H$. Therefore $b_2H$ is a third right coset of H such that $b_2H$, $b_1H$, and H are distinct right cosets. If $b_2h_i = b_1h_j$ for some $i$ and $j$, then $b_2 = b_1h_jh_i^{-1}$. Similarly if $b_2h_i = h_j$, then $b_2 = h_jh_i^{-1}$. In both cases this is contrary to the choice of $b_2$. Again there are two cases, either $g = 3h$, or $g > 3h$. If $g = 3h$, then the theorem is proved. If $g \quad 3h$, then continue by finding a distinct element $b_3$ of G not in any right coset previously determined and form a fourth right coset. Continue the process until a $k$ is found such that if $g > (k-1)h$, then $g = kh$. Thus the proof of the theorem is completed.

It follows from the proof of the theorem that the number of right cosets is g/h = k where g is the order of G and h is the order of H. This number k is called the index of H in G.

Definition 3: If every element of a group g can be expressed as a product of powers of elements in a subset of G, then the subset is said to generate G.

If S is a set of generating elements of a group G, and if no element of S can be expressed as a product of powers of the remaining elements of G, then S is said to be a set of independent generators.

Theorem 3: Every group G possesses a set of independent generators.

Proof: Let the set of elements I, b, ...., n be the set of all of the elements of G. The element I can be removed since it is the product of any element and its inverse. Now, either the remaining elements in the set form an independent set of generators or they do not. If they do, then no element can be expressed as a product of the remaining ones. Thus the theorem is proved. On the other hand if the remaining elements do not form an independent set of generators, then some other element, say a, can be expressed as a product of the others. Then either the set of elements with I and a deleted is a set of independent generators, or it is not. If it is, then the theorem is proved. If not, continue the process until a set of independent generators is found, and the theorem is proved.

The defining relations of a group indicate the orders of the generators of the group and the relations between them.

As a result of Theorem 3 the cyclic group is generated by a single element, for every element of G can be expressed as a power of a, where a is the single element.

Let $a_1, a_2, \ldots, a_n$ be a given set of elements. Then the notation $\{a_1, a_2, \ldots, a_n\}$ is used to denote the group that arises from every possible product of the given elements. For example the cyclic group of order n can be denoted by $\{a\}$.

Theorem 4: The order of an element of a group G is a factor of the order of G.

Proof: If m is the order of an element a of G, then $a^m = I$, defines the cyclic group of order m. Hence it follows from Theorem 2 that m is a factor of the order of G.

Conjugate Elements and Subgroups

Consider the elements a, b, and t of a group G. If $t^{-1}at = b$, then t is said to transform a into b. If a = b, then a is said to be invariant or self-conjugate under t. That is, if $t^{-1}at = a$, then a commutes with every element t of G.

Definition 4: If the elements a and t are elements of a group G, then a and $t^{-1}at$ are said to be conjugate elements of G.

Theorem 5: If a and $t^{-1}at$ are two conjugate elements of a group G, then $(t^{-1}at)^m = t^{-1}a^m t$.

Proof:
$$\begin{aligned}(t^{-1}at)^m &= t^{-1}att^{-1}at\ldots t^{-1}at\\ &= t^{-1}a^2tt^{-1}at\ldots t^{-1}at\\ &= \ldots\\ &= t^{-1}a^m t.\end{aligned}$$

Theorem 6: Two elements which are conjugate in a given group have the same order.

Proof: Let a be an element of order n, and t any other element of G. Then from Theorem 5

$$\begin{aligned}(t^{-1}at)^n &= t^{-1}a^nt\\ &= t^{-1}It\\ &= I.\end{aligned}$$

Conversely if $t^{-1}at$ is of order n, then

$$\begin{aligned}a^n &= t(t^{-1}a^nt)t^{-1}\\ &= t(t^{-1}at)^nt^{-1}\\ &= tIt^{-1}\\ &= I.\end{aligned}$$

Thus the theorem is proved.

Let $t^{-1}Ht$ be the set of conjugates of the elements of H under t. It can be shown that this is a subgroup.[1]

Definition 5: If H is a subgroup of a group G, and t is an element of G, then H and $t^{-1}Ht$ are called conjugate subgroups of G.

The subgroup H is said to be transformed into $t^{-1}Ht$ by the element t. If t is an element of H, then every subgroup tH of G is conjugate to itself, since it can be transformed into itself by each of its own elements. If the

[1] Robert D. Carmichael, Groups of Finite Order, Ginn and Company, 1937. p. 47.

subgroups H and $t^{-1}Ht$ are identical for every $\underline{t}$ of G, then H is said to be a self-conjugate or an invariant subgroup of G.

Definition 6: The center of a group G is the subgroup whose elements transform each element of G into itself.

In the proof of Lagrange's theorem if H is self-conjugate, then the cosets form a group. This group is called the quotient group and is denoted by G/H. Its order is equal to the index of H in G.

## Direct Products

The following theorem is essential in determining the number of groups of certain orders.

Theorem 7: If two groups H and K have no element in common except the identity, and if every element of H commutes with every element in K; then the set H,K is a group of order hk.

Proof: If $h_i$ belongs to H and $k_j$ belongs to K, where $i = 1, \ldots, h$ and $j = 1, \ldots, k$; then there exist hk elements of the form $h_i k_j$. Since every element $h_i k_j = k_j h_i$ and since H and K are groups, the set is closed. The associative law holds for it holds in H and K. The identity element belongs to the set since it is in both H and K. Also every element has an inverse for the set contains every element in the two groups. Therefore the set forms a group and from the first sentence in this proof, the group is of order hk. Hence the theorem is proved.

Definition 7: The group in theorem 7 is called the direct product of H and K.

## Isomorphisms

Suppose there are two groups G and H both of order n. Let $a_1$, $a_2$, ..., $a_n$ and $b_1$, $b_2$, ..., $b_n$ be the elements of G and H respectively. If the elements with the same subscripts correspond to each other, and if $a_ia_j \leftrightarrow b_ib_j$ for all i and j, then the two groups G and H are said to be isomorphic.

Now suppose one wants to obtain all possible groups of a given order. If the defining relations between two of these groups are the same, then these two groups are isomorphic. As a simple example consider the two groups of order 4, one being the group defined by the integers (mod 4) under addition, and the other by the elements (1, i, -1, -i) under the operation of multiplication, where i is the complex number defined in the usual manner. The isomorphism established between the two groups is more easily seen if a table of the elements is set up as follows:

|   | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

|   | 1 | i | -1 | -i |
|---|---|---|---|---|
| 1 | 1 | i | -1 | -i |
| i | i | -1 | -i | 1 |
| -1 | -1 | -i | 1 | i |
| -i | -i | 1 | i | -1 |

The relationship between the element 0 ↔ 1; 1 ↔ i; 2 ↔ -1; and 3 ↔ -i of the respective groups indicates that the first condition for an isomorphism holds. To show that operations are preserved one only needs to observe from the two tables that $a_ia_j \leftrightarrow b_ib_j$ holds for every element.

## Sylow's Theorem and Consequences

The first two of the following three theorems are quoted because their results are needed in a later proof. The most important Sylow Theorem is quoted and not proved because of the length of its proof. The third theorem enables one to determine the number of subgroups whose order is the power of a prime. This concept is extremely important in the development of the possible groups of a given order.

Theorem 8: The elements of a finite group G which commute with a given element $g_1$ in G form a subgroup H of G. The number of elements conjugate to $g_1$ in G is equal to the index of H in G.[1]

Theorem 9: The elements of a finite group G which commute 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 self-conjugate subgroup. The number of subgroups conjugate to H in G is equal to the index of K in G.[2]

Theorem 10 (Sylow's): Let G be a group of order n and let $p^m$ be the highest power of a prime p contained in n as a factor, m being a positive integer. Then G contains at least one subgroup of order $p^m$. All its subgroups of order $p^m$ form a single complete conjugate set, and their number is 1+kp, where k is an integer (positive or zero).[2]

The subgroup referred to in Theorem 10 is called a Sylow subgroup.

In the proof of Sylow's Theorem the following corollary was proved.[3]

[1] Carmichael, Robert D., Groups of Finite Order, Ginn and Company, 1937, p. 48.

[2] Ibid., p. 49.

[3] Ibid., p. 58.

Corollary 1: The only elements of G which commute with a Sylow subgroup of G of order $p^a$ and whose orders are powers of $\underline{p}$, are the elements of that Sylow subgroup.[1]

Corollary 2: The number 1+kp of Sylow subgroups of G of order $p^m$ is a factor of the order of G.

Proof: From Theorem 9 the number of subgroups conjugate to H in G is equal to the index of K in G which is a factor of the order $\underline{g}$ of G. Since the Sylow subgroups of order $p^m$ form a complete set of conjugate subgroups of G, this number 1+kp must be a factor of the order of G, and the corollary is proved.

## Prime Power Groups

Definition 8: A prime power group is a group whose order is a power of a prime.

Let G be a group whose order is not a power of a prime. Then if $\underline{n}$ is the order of G, $n = p_1^{m1}p_2^{m2}\ldots p_r^{mr}$. There are at least two primes contained in $\underline{n}$. Thus from Sylow's Theorem G contains two or more prime power subgroups, for if $p_1$ and $p_2$ are factors of $\underline{n}$, then there exists $1+k_1p_1$ subgroups of order $p_1^{m1}$, and $1+k_2p_2$ subgroups or order $p_2^{m2}$, where $k_1$ and $k_2$ are non-negative integers. A given group may be generated by a set of Sylow subgroups; for if this set contains one Sylow subgroup of each order, then for each Sylow subgroup there exists a set of generators. These generators determine a group whose order is at least as great as that of the given group, and hence the group so generated

[1] Carmichael, Robert D., Groups of Finite Order, Ginn and Company, 1937, p. 63.

coincides with the given group. This fact alone shows the importance of prime power groups.

Theorem 11: A prime power group G of order $p^m$ contains a self-conjugate element of order $p$.

Proof: When G is Abelian, then every element in G is self-conjugate, and hence the theorem is true. Then suppose G is non-Abelian. Let $a$ be an element of G which is not self-conjugate, and consider the complete set of conjugates to which $a$ belongs. From Theorem 8 it follows that the number of conjugates of $a$ is a factor of $p^m$, and hence the number is $p^r$ where $r$ is some positive integer. Therefore the elements of G which are not self-conjugate fall into sets, each containing a number of elements which is divisible by $p$. Since no two of these sets have an element in common, it follows that the number of elements in G which are not self-conjugate is a multiple of $p$, say ip. But the number of elements in G besides the identity is $p^m-1$. Let $k$ be the number of self-conjugate elements in G besides the identity. Then $k+ip = p^m-1$ implies that $k+1 = p(p^{m-1}-i)$, and it follows that k+1 is divisible by $p$. If $k = 0$, this conclusion is not valid. Hence G contains a self-conjugate element besides the identity, and the order of such an element is necessarily a power of $p$. Therefore the theorem follows.

Corollary 1: The number of self-conjugate elements of G is a power of $p$.

Proof: From the above theorem all distinct powers of the self-conjugate element are self-conjugate. Hence the number of self-conjugate elements is a power of $p$.

Corollary 2: A group H of order $p^2$ is Abelian.

Proof: If H contains an element of order $p^2$, it is cyclic, and hence Abelian. If H is not cyclic, let *a* be a self-conjugate element of order *p* and let *b* be an element of H which is not in $\{a\}$. Then $b^{-1}ab = a$ which implies $ab = ba$. From Theorem 4 the element *b* is also of order *p*. Therefore H is the direct product $\{a,b\}$ of $\{a\}$ and $\{b\}$, and $\{a,b\}$ is Abelian.

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

Proof: From Sylow's Theorem it follows that G contains a subgroup of order *p*. Hence from the theorem just proved, G contains an element of order *p*. Thus the corollary is proved.

## Groups of Order pq

Suppose G is of order pq, where *p* and *q* are primes. Let *p* be less than *q*. Then from Sylow's Theorem the number of subgroups of order *q* is of the form 1+kq. The second corollary of Sylow's Theorem indicates that this number divides pq. Hence there is only one subgroup of order *q* since *p* *q*, and *q* is the order of the unique cyclic group $\{b\}$ defined by $b^q = I$. The number of subgroups of order *p* is of the form 1+kp and divides pq, and thus must be 1 or *q*. If the number of subgroups of order *p* is 1, then there exists a self-conjugate subgroup $\{a\}$ defined by $a^p = I$. Consequently, G is the direct product of a and $\{b\}$. Here $c = ab$ is of order pq, and G is cyclic. There remains the case with $1+kp = q$ subgroups of order p, where a subgroup $\{a\}$ of order *p* is not self-conjugate. Then

$$a^p = I; \; b^q = I.$$

Since $\{b\}$ is self-conjugate, $a^{-1}ba = b^r$, for some $\underline{r}$. Here if $r = 1$, $G$ is Abelian, and it is the cyclic group named above. Hence in order to have a new group, $r \neq 1$. Then $a^{-1}b^i a = b^{ir}$ for any $\underline{i}$, and in particular $a^{-1}b^r a = b^{r^2}$. Hence $a^{-2}ba^2 = a^{-1}b^r a = b^{r^2}$. Proceeding by induction it is assumed that this is true for j-1. Thus

$$a^{-j+1}ba^{j-1}b^{r^{j-1}}$$

$$a^{-1}a^{-j+1}ba^{j-1}a = a^{-j}ba^{j} = a^{-1}b^{r^{j-1}}a = b^{r^j}.$$

For $j = p$, this becomes $b = a^{-p}ba^{p} = b^{r^p}$. Since $\underline{b}$ is of order q, $r^p \equiv 1$ (mod q). Then the complete set of defining relations is

1.) $a^p = b^q = I$; $ba = ab^r$.

If $r^p \equiv 1 \pmod q$ has only the solution $r = 1$, then there exists only one abstract group of order pq. If $r = 1$, $a^{-1}ba = a$ implies that $ba = ab$. This is the cyclic group named above. Thus in order for there to be more than one group of order pq, $r^p \equiv 1 \pmod q$ must have more than one solution.

The condition will now be determined in which the equation $r^p \equiv 1 \pmod q$ has more than one solution. Using the index theory one can change

$$r^p \equiv 1 \pmod q$$

into $$p(\text{ind } r) \equiv 0 \pmod{q-1}.$$

If $\underline{p}$ divides q-1, then let $p = k(q-1)$ so that

$$\text{ind } r \equiv 0 \pmod k.$$

This will have more than one solution for $\underline{r}$ mod q. Therefore the condition has been established. Hence the following two relationships exist for abstract groups of order pq.

1.) $a^{pq} = I$.

2.) $a^p = b^q = I$; $ba = ab^r$, $r \not\equiv 1 \pmod q$ where $\underline{p}$ divides $q-1$.

## Abelian Groups

An Abelian group can have only one Sylow subgroup of a given order since all the Sylow subgroups are conjugate under every group. Hence every Abelian group is the direct product of its Sylow subgroups whenever its order is divisible by more than one prime number. Then a necessary and sufficient condition that two Abelian groups are isomorphic is that their Sylow subgroups are isomorphic. Hence the study of Abelian groups is reduced to the study of groups whose orders are powers of a single prime number because the order of a Sylow subgroup is a power of a prime. In particular if the order of an Abelian group is not divisible by the square of a prime number, the group must be cyclic. If pq is the order of the group G, then from the section on groups of order pq there exists only one Abelian group of order pq, namely the cyclic group.

The abstract four-group has the elements, I, a, ab, b, with the following multiplication table:

| | I | a | ab | b |
|---|---|---|---|---|
| I | I | a | ab | b |
| a | a | I | b | ab |
| ab | ab | b | I | a |
| b | b | ab | a | I |

The symmetric multiplication table indicates that the group is Abelian. Also

The table shows that any one of the three non-identity elements combined with the identity element forms a cyclic group of order two, (i.e. The two elements form a subgroup of the four-group). This result helps in part to prove the following theorem.

Theorem 12: If the order *n* of an Abelian group G is divisible by an integer *m*, G contains a subgroup of order *m*.

Proof: The example preceeding this theorem shows that the theorem is true when n = 4. Mathematical induction will be used to prove it in general. Assume it is true for all orders less than *n*. Let *p* be a prime factor of *m*. Since G is an Abelian group each of its subgroups must not only be self-conjugate, but also Abelian. So G contains a self-conjugate subgroup, say H, of order *p*. Now the Abelian quotient group G/H has order n/p which is less than *n*. By induction it contains a subgroup of order m/p and to this subgroup of G/H corresponds a subgroup of order *m* in G, which completes the proof of the theorem.

Theorem 13: An Abelian group whose order is not a power of a prime number is the direct product of all its Sylow subgroups.

Proof: Since all Sylow subgroups of a given order in a finite group G form a single complete conjugate set, it follows that a given Abelian group can have only one Sylow subgroup of a given order. Since no two of these subgroups have an element in common except the identity, the theorem follows.

Lemma 1: If $g_1$ is the element of largest order, $p^{m_1}$, in a prime-power group G, and if $g_r$ is any other element of G, then $g_r^{p^{m_2}}$ is contained in the cyclic group generated by $g_1$.

Proof: The order of $g_r$ is a power of p, for the elements, I, $g_r$, $g_r^2$, $g_r^3$, ...., $g_r^{p^{m_2}} = I$, form a subgroup of G. Hence from Lagrange's Theorem the order of the subgroups of G is a factor of $p^m$, where $p^m$ is the order of G. Since $p^{m_2}$ is the order of $g_r$, and from the hypothesis $m_2 \leqq m_1$, then

$$g_r^{p^{m_1}} = ((g_r)^{p^{m_2}})^{p^{m_1-m_2}} = (I)^{p^{m_1-m_2}} = I.$$

Thus the lemma is proved, for I is certainly contained in $\{g_1\}$.

Theorem 14: A non-cyclic Abelian group G whose order is a prime power, say $p^m$, is the direct product of independent cyclic groups.

Proof: From the lemma every element of G raised to the $(p^{m_1})$th power is in $\{g_1\}$. Choose $m_2$ such that the $(p^{m_2})$th power of any element in G belongs to $\{g_1\}$, but the $(p^{m_2-1})$th power of some element in G, say $a_2$ does not belong to $\{g_1\}$. Since $\{g_1\}$ is cyclic and G contains no element of order greater than $p^{m_1}$, it follows that every element which is in $\{g_1\}$ and is the $(p^{m_2})$th power of an element of G is a $(p^{m_2})$th power of an element in $\{g_1\}$. Let $a_2'$ be in $\{g_1\}$ whose $(p^{m_2})$th power of $a_2'a_2$ is in $\{g_1\}$ since such a power is the product of two factors, one of which belongs to $\{g_1\}$ while the other does not. Then set $a_2'a_2 = g_2$. Then $\{g_2\}$ is the second of the cyclic groups named in the theorem, for $(a_2'a_2)^{p^{m_2}} = I$.

The direct product $\{g_1, g_2\}$ of $\{g_1\}$ and $\{g_2\}$ is either G, or it is not. If so, the theorem is proved; and if not, let $m_3$ be such that the $(p^{m_3})$th power of every element of G is in $\{g_1, g_2\}$, while G contains an element $a_3$ whose $(p^{m_3-1})$th power is not in $\{g_1, g_2\}$. Then there is an element $a_3'$ in $\{g_1, g_2\}$ whose $(p^{m_3})$th power is the inverse of the $(p^{m_3})$th power of $a_3$. Let $a_3'a_3 = g_3$. Then the element $g_3$ is of order $p^{m_3}$, while no power of $g_3$ lower than the $(p^{m_3})$th is in $\{g_1, g_2\}$. Thus $\{g_3\}$ is the third cyclic group named in the theorem. Hence the direct product of $\{g_1, g_2\}$ and $\{g_3\}$ is $\{g_1, g_2, g_3\}$. Again $\{g_1, g_2, g_3\}$ is G, or it is not. If not repeat the process until G can be expressed as $\{g_1, g_2, \ldots, g_k\}$, a direct product of k cyclic groups, as demanded in the theorem.

If the concept of the direct product is extended to the direct product of several groups, and if $p^{m_i}$ is the order of the (i)th such group, then one observes that

$$p^m = p^{m_1}p^{m_2}\ldots p^{m_k}$$

$$= p^{m_1+m_2+\ldots+m_k}.$$

Thus $$m = m_1+m_2+\ldots+m_k.$$

Hence the following definition is stated.

Definition 9: If the orders of $g_1$, $g_2$, ..., $g_k$ are $p^{m_1}$, $p^{m_2}$, ..., $p^{m_k}$ respectively, then G is said to be of type $(m_1, m_2, \ldots, m_k)$.

Corollary 1: The number of abstract Abelian of order $p^m$ equals the number of distinct integral partitions of m, each partition giving rise to a distinct type.

Proof: This corollary follows immediately from the theorem and Definition 9.

## POSSIBLE ABSTRACT GROUPS OF GIVEN ORDER

The theory that has been developed can now be applied to determine the number of abstract groups of a given order. Since many of the developments are similar, it will be sufficient to determine only a few of them in this paper. It follows from Theorem 11, Corollary 2, that there exist only Abelian groups of order $p^2$, where p is prime. From the Corollary of Theorem 14 there are only two abstract groups of order $p^2$ since there are only two partitions of the integer 2.

The groups of orders 12, 18, and 20 have orders of the form $p^2q$, where p and q are primes. The abstract groups of order 12 will be determined. A similar procedure can be followed to determine the abstract groups of orders 18 and 20 respectively.

The groups of prime order are determined by the following theorem.

Theorem 15: There exists only one abstract group G whose order is prime p.

Proof: From Theorem 4 the order of an element of G is a factor of the order of G. However, the only factors of p are 1 and p. If the factor is p, then the subgroup is cyclic with order p. Therefore this is the only group.

The order of the groups of order 24 is of the form $p^3q$ where p and q are primes. Since they are of a different type than the other groups of order 1 through 26, they will be determined. Finally, the results of the section on groups of order pq will be used to complete the table of abstract groups of order 1 through 26.

## Groups of Order 8

Since 3 can be partitioned into (3), (2, 1), and (1, 1, 1), there are three Abelian types of order 8. They have the following defining relations.

1.) $a^8 = I$.

2.) $a^2 = b^4 = I$; $xy = yx$, where $x, y = a, b$.

3.) $a^2 = b^2 = c^2 = I$; $xy = yx$, where $x, y = a, b, c$.

A non-Abelian group of order 8 cannot contain elements of order 8 for that is the cyclic group which has already been determined. If all the elements are of order 2, then

$$(ab)^2 = abab = I.$$

$$ab = a(I)b = a(abab)b = a^2bab^2 = ba,$$

and the group is Abelian. Hence there must be an element of order 4, say $a^4 = I$. If $\underline{b}$ belongs to the subgroup $\{a\}$, then G is $\{a,ab\}$, and $b^2$ belongs to $\{a\}$. If $b^2 = a$ or $a^3$, then $\underline{b}$ is of order 8, for

$$I = a^4 = (b^2)^4 = b^8,$$

or

$$b^8 = (b^2)^4 = (a^3)^4 = (a^4)^3 = I,$$

and G is cyclic. Hence $b^2 = I$ or $a^2$, so $b^4 = I$. Since $a$ is self-conjugate, $b^{-1}ab$ belongs to $\{a\}$ and $b^{-1}ab = a$ or $a^3$. But if $b^{-1}ab = a$, then $ab = ba$, and G is Abelian. Thus $b^{-1}ab = a^3$. Consequently there are two non-Abelian groups of order 8. One generated by the relations

4.) $a^4 = b^2 = I$, $ab = ba^3$,

which is called the dihedral group. The other group is generated by

5.) $a^4 = I$; $b^2 = a^2$; $ab = ba^3 = b^3a$,

which is called the quaternion group. Thus there exist five abstract groups of order 8.

## Groups of Order 12

The Abelian groups of order 12 are determined by taking the direct product of the groups of order 4 and the group of order 3. Since there are just two groups of order 4, both Abelian, then there are 2 Abelian groups of order 12. They are defined by

1.) $a^3 = b^4 = I$; $ab = ba$.

2.) $a^3 = b^2 = c^2 = I$; $xy = yx$, where $x, y = a, b, c$.

Now suppose the group of order 4 is cyclic. This cyclic group is either self-conjugate, or it is not. If it is, let b be the element which generates it. Also let a be an element of order 3 such that $a^3 = I$. Then

$$a^{-1}ba = b^r$$

$$a^{-3}ba^3 = b^{r^3}$$

$$b^{r^3} = b$$

$$r^3 \equiv 1 \pmod 4$$

$$r \equiv 1 \pmod 4.$$

It follows that a commutes with b, and hence G is an Abelian group. Then since all of the Abelian groups have been determined, no new groups are determined.

Consider the case where the cyclic group of order 4 is not self-conjugate.

Then $b^2$ is a self-conjugate element, and $\{a\}$ is also self-conjugate. Hence

$$b^{-1}ab = a^r$$

$$b^{-4}ab^4 = a^{r^4}$$

$$a = a^{r^4}$$

$$r^4 \equiv 1 \pmod 3)$$

$$r \equiv 1,\ 2 \pmod 3).$$

If $r \equiv 1$ (mod 3), then one obtains the cyclic group of order 12. Hence $r \equiv 2$ (mod 3) is the only new result.

3.) $a^3 = b^4 = I;\ ab = ba^2.$

Now suppose the group of order 4 is the four-group. Either it is self-conjugate, or it is not. If it is, then

$$a^{-1}ba = b,\ bc,\ \text{or } c.$$

If $a^{-1}ba = b$, then the group is Abelian and has already been determined. If $a^{-1}ba = bc$, and if $a^{-2}ba^2 = c$, then by eliminating $\underline{c}$ from these two relations, the following result is obtained.

$$ba^2ba = aba^2$$

$$ba^2ba^2 = ab$$

$$a^2ba^2ba^2 = b$$

$$a^2ba^2ba^2b = I$$

$$(a^2b)^3 = I.$$

Thus the new group is defined by the following relations.

4.) $a^3 = (a^2b)^3 = b^2 = I.$

This group is called the alternating group of degree 4.

Thus in order to obtain a new group, the four-group is not self-conjugate. Then the self-conjugate group of order 2 is either $\{b\}$ or $\{c\}$. Consequently, if a is an element of order 3, it must be one of two conjugate elements while $\{a\}$ is self-conjugate. Thus

$$bab = a;\ cac = a^r$$

and

$$cac = a^r;\ bab = a.$$

The second relationship is simply the first with b and c interchanged. Now

$$b^2ab^2 = a^{r^2}$$

$$IaI = a^{r^2}$$

$$a = a^{r^2}$$

$$r^2 \equiv 1 \pmod 3$$

$$r \equiv 1,\ 2 \pmod 3.$$

Hence a new group is defined by

5.) $a^3 = b^2 = c^2 = I;\ ab = ba^2;\ xy = yx,$ where $x = a,\ b$ and $y = c.$

Thus there are five abstract groups of order 12.

## Groups of Order 24

From Sylow's Theorem a group of order $24 = 3(2^3)$ must contain either 1 or 3 subgroups of order 8. Such a group may also have 1 or 4 subgroups of order 3. If it has one subgroup of order 8 and one subgroup of order 3, the group must be their direct product, since from Sylow's Theorem each of these subgroups is self-conjugate. From the discussion on groups of order 8, it was observed that there are five abstract groups of this order. Therefore there are five distinct groups of order 24 each of which is obtained by taking the direct product of the group of order 3 and one of the five groups named in the other section. These five groups have the following defining relations.

1.) $a^3 = b^8 = I$; $ab = ba$.

2.) $a^3 = b^4 = c^2 = I$; $xy = yx$, where $x, y, = a, b, c$.

3.) $a^3 = b^2 = c^2 = d^2 = I$; $xy = yx$, where $x, y = a, b, c, d$.

4.) $a^3 = b^4 = c^2 = I$; $bc = cb^3$; $xa = ax$, where $x = b, c$.

5.) $a^3 = b^4 = c^4 = I$; $bc = cb^3$; $xa = ax$, where $x = b, c$.

If there are three subgroups of order 8, some two of them must have a common subgroup of order 4; and this common subgroup must be a self-conjugate subgroup of the group of order 24. Moreover if, in this case, a subgroup of order 8 is Abelian, each element of the self-conjugate subgroup of order 4 must be a self-conjugate element of the group of order 24.

Now suppose a group of order 8 is cyclic and let <u>b</u> be the element which generates it. If b is self-conjugate and <u>a</u> is an element of order 3, then

$$a^{-1}ba = b^{r}$$

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

$$= a^{-1}b^{r^{2}}a = b^{r^{3}}$$

$$r^{3} \equiv 1 \pmod{8}$$

$$r \equiv 1 \pmod{8}.$$

Consequently, the above relation $a^{-1}ba = b$ implies that $ab = ba$. This is the abstract group 1.) already obtained. Hence $\{b\}$ cannot be self-conjugate, and $b^{2}$ must be a self-conjugate element. Therefore a is one of two conjugate elements while $\{a\}$ is self-conjugate. Hence, the following relations determine a new group.

6.) $a^{3} = b^{8} = I$; $ab = ba^{2}$.

Next let a group of order 8 be an Abelian group defined by $b^{4} = c^{2} = I$; $bc = cb$. If this is self-conjugate, then by considerations similar to those given above, it is inferred that the group is the direct product of groups of order 8 and 3, and hence has already been determined.

If the group of order 8 is not self-conjugate, the self-conjugate group of order 4 may be either $\{b\}$ or $\{b^{2}, c\}$. In either case if a is an element of order 3, it must be one of two conjugate elements while $\{a\}$ is self-conjugate. Hence there are two new groups defined by

7.) $a^{3} = I$; $cac = a^{2}$; $b^{-1}ab = a$.

8.) $a^{3} = I$; $b^{-1}ab = a^{-1}$; $cac = a$.

Let a group of order 8 be the Abelian group defined by $b^2 = c^2 = d^2 = I$; $xy = yx$, where $x, y = b, c, d$. If it is self-conjugate, and if the group of order 24 is not the direct product of groups of orders 8 and 3, then an element $a$ of order 3 must transform the 7 elements of order 2 among themselves. Therefore $a$ must commute with one of these 7 elements. Now the second relation below

$$a^{-1}ba = b;\ a^{-1}ca = bc$$

is not self consistent, because the two imply that

$$a^{-2}ca^2 = a^{-1}(a^{-1}ca)a$$

$$= a^{-1}bca$$

$$= a^{-1}baa^{-1}ca$$

$$a^{-2}ca^2 = bbc$$

$$= c.$$

Therefore $$a^{-1}(a^{-2}ca^2)a = c = a^{-1}ca.$$

Hence, since the group of order 8 is generated by $b$, $c$ and any other element of order 2 except $bc$, it may be assumed without loss of generality, that

$$a^{-1}ba = b;\ a^{-1}ca = d;\ a^{-1}da = b^xc^yd^z,$$

where $x$, $y$, and $z$ are positive integers. These relations give

$$c = IcI = a^{-3}ca^3$$

$$= a^{-2}a^{-1}caa^2$$

Continuing

$$c = a^{-2}da^{2}$$

$$= a^{-1}(a^{-1}da)a$$

$$= a^{-1}(b^{x}c^{y}d^{z})a$$

$$= a^{2}(b^{x}c^{y}d^{z})a$$

$$= b^{x}a^{2}c^{y}d^{z}a.$$

Now

$$a^{2}c^{y}a = d^{y}$$

$$a^{2}c^{y} = d^{y}a^{2},$$

and

$$a^{2}d^{z}a = (b^{x}c^{y}d^{z})^{z}$$

$$a^{2}d^{z} = (b^{x}c^{y}d^{z})^{z}a^{2}.$$

Thus

$$c = b^{x}d^{y}a^{2}d^{z}a$$

$$= b^{x}d^{y}b^{xz}c^{yz}d^{z^{2}}a^{2}a$$

$$= b^{x(1+z)}c^{yz}d^{y+z^{2}}$$

$$= c.$$

Now $yz = 1$, since *y* and *z* are positive integers, then

$$y = z = 1.$$

Now if

$$a^{-1}da = bcd,$$

and if

$$bc = c', \; bd = d',$$

then $$a^{-1}c'a = d',\ a^{-1}d'a = b'd';$$

so that the two alternatives $x = 0$ and $x = 1$ lead to isomorphic groups. By choosing $x = 0$, a new group is obtained. It is the direct product of $\{b\}$ and $\{a, c, d\}$ where

9.) $a^{-1}ca = d;\ a^{-1}da = cd.$

If the group of order 8 is not self-conjugate, the self-conjugate group of order 4 may be taken to be $\{b,d\}$. If $\underline{a}$ is an element of order 3, then there is a single new abstract group given by

10.) $a^3 = I;\ dad = a^2;\ bab = a;\ cac = a.$

Let a group of order 8 be defined by the non-Abelian group defined by

$$b^4 = c^4 = I;\ c^{-1}bc = b^{-1},$$

and let $\underline{a}$ be an element of order 3. If the group of order 8 is self-conjugate and the group of order 24 is not a direct product of groups of orders 8 and 3, $\underline{a}$ must transform the 3 subgroups of order 4, $\{b\}$, $\{c\}$, and $\{bc\}$, among themselves. Hence

$$a^{-1}ba = c$$

and

$$a^{-1}ca = bc \text{ or } (bc)^3.$$

If $\underline{a}$ transforms $\underline{c}$ into $(bc)^3$, then

$$a^{-3}ca^3 = b^{-1},$$

and $\underline{a}$ cannot be an element of order 3. Hence in this case there is only one new abstract group.

11.) $a^3 = I$; $a^{-1}ba = c$; $a^{-1}ca = bc$.

If the subgroup of order 8 is not self-conjugate, the self-conjugate subgroup of order 4 is cyclic, and each of its elements must commute with $a$. Hence again there is one new abstract group.

12.) $a^3 = I$; $b^{-1}ab = a$; $c^{-1}ac = a^2$.

Finally, let a subgroup of order 8 be a non-Abelian group defined by

$$b^4 = c^2 = I; \; cbc = b^3.$$

This contains one cyclic and two non-cyclic subgroups of order 4. If it is self-conjugate, the group of order 24 must therefore be the direct product of groups of orders 8 and 3; and there is no new abstract group.

If the subgroup of order 8 is not self-conjugate, and the self-conjugate subgroup of order 4 is the cyclic group $\{b\}$, then $b$ must commute with an element $a$ of order 3, and there is a single new abstract group given by

13.) $a^3 = I$, $b^{-1}ab = a$, $c^{-1}ac = a^2$.

If the self-conjugate subgroup of order 4 is not cyclic, it may be taken to be $\{I, b^2, c, b^2c\}$. If $a$ commutes with each element of this subgroup, there is a single abstract group given by

14.) $a^3 = I$, $b^{-1}ab = a^2$, $a^{-1}ac = a$

If $a$ does not commute with every element of the self-conjugate subgroup, it must transform $b^2$, $c$, $b^2c$ among themselves and then $a^{-1}b^2a = c$, $a^{-1}ca = b^2c$.

Now $\{c, a^2, b\}$ is self-conjugate, and therefore $a$ must transform $c$ into another element of order 3 contained in this subgroup. Hence $b^{-1}ab = a^xb^{2y}c^z$.

The only values of $x$, $y$, and $z$ which are consistent with the previous relation $b^2ab^2 = ab^2a$, are

$$x = 2, \; y = z = 1.$$

The last new group is therefore defined by

$$a^3 = I; \; a^2b^2a = c; \; a^2ca = b^2c; \; b^{-1}ab = a^2b^2c.$$

When $\underline{c}$ is eliminated between these relations, it will be found that the only independent relations remaining are

15.) $a^3 = b^4 = (ba)^2 = I.$

Then

$$\begin{aligned}(ba)(ba) &= b(ab)a = b^2a^2b^2ca \\ &= b^2ca^2ca \\ &= b^2cb^2ca^2a \\ &= b^2cb^2c \\ &= (a^2ca)a^2ca \\ &= a^2c^2a \\ &= I.\end{aligned}$$

Therefore there are 15 abstract groups of order 24.

## Conclusion

It follows from the section on groups of order pq that there are two abstract groups of orders 6, 10, 14, 21, 22, and 26 respectively. Since 3 does not divide 4, there is only one abstract group of order 15. Hence all of the groups of order pq through 26 have been determined.

The order of the groups of order 9 and 25 is of the form $p^2$, and hence from Corollary 2 or Theorem 11 there are two abstract groups.

The following table summarizes this section.

| Order | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16[1] | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 5 | 2 | 2 | 1 | 5 | 1 | 2 | 1 | 14 | 1 | 5 | 1 | 5 | 2 | 2 | 1 | 15 | 2 | 2 |

[1] Burnside, W., Theory of Groups, Macmillan Company, 1897, p. 87.

# ACKNOWLEDGMENT

The author wishes to express his thanks and appreciation to his major professor, Dr. Leonard E. Fuller, for the valuable suggestions and assistance which he so patiently gave; thus, he made this paper possible.

# BIBLIOGRAPHY

1. Alexandroff, P. S., Introduction to the Theory of Groups, Hafner Publishing Company, New York, 1959.

2. Benner, Charles P., and others, Topics In Modern Algebra, Harper Brothers, New York, 1962.

3. Birkhoff, Garrett and MacLane Saunders, Survey of Modern Algebra, Macmillan company, New York, 1941.

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

5. Carmichael, Robert D., Groups of Finite Order, Ginn & Company, New York, 1937.

6. Fuchs, L., Abelian Groups, Pergamon Press, London, 1960.

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

8. Kurosh, The Theory of Groups, New York Publishing Company, New York, 1955.

9. MacDuffee, Cyrus Colton, An Introduction To Abstract Algebra, John Wiley & Sons, Inc., New York, 1940.

10. Mathewson, Louis Clark, Elementary Theory of Finite Groups, Houghton Mifflin Company, New York, 1930.

11. Miller, George A., Blichfeldt, H. F., Dickson, L. E., Finite Groups, John Wiley & Sons, Inc., New York, 1916.

12. Miller, Kenneth S., Elements of Modern Abstract Algebra, Harper and Brothers Publishers, New York, 1958.

# DETERMINATION OF GROUPS OF ORDERS 1 THROUGH 26

by

RONNIE LEE YARROW

B. S., Kansas State University, 1961

---

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

1963

# ABSTRACT

In this paper the abstract groups of orders 1 through 26 are determined. The theory involved greatly reduces the labor of testing the group postulates in each case. This gives insight on methods that can be used should one desire to determine the groups of orders greater than 26.

These groups are obtained by breaking down the order into prime power factors. Since the order of a subgroup is a factor of the order of the group, subgroups are used to determine the respective groups. Sylow's theorem and corollaries are used to determine the number of subgroups of the respective orders. If there is but one Sylow subgroup of each possible order, then the group is formed by taking the direct product of these respective subgroups. The Abelian groups are determined by taking the direct product of Abelian subgroups. A subgroup is either self-conjugate or it is not. If so, then every element of the group must transform this subgroup into itself. This gives a relationship between each of the elements of the group. If the subgroup is not self-conjugate, then some of the elements of the group are; and again there is a relationship between the elements of the group. The important fact is that there is a relationship between the elements of a group, and conjugate theory provides a means of finding this relationship.

The special types of groups determined are those which have orders $p^2$, pq, and p respectively. There are always two groups of order $p^2$, one cyclic and the other Abelian. If p divides q-1, there are two groups of order pq. The first is the cyclic group, and the second is non-Abelian. There exists only one group of order p which is the cyclic group.

The procedure for finding groups of order $p^2q$ is similar for different p and q. However, in each case it is necessary to go through the process

of determining the results, as they are not always the same. Similarly, the same is true for groups of order $p^3q$. There exist 5 groups of order $p^3$ where $p = 2$.