SOME GROUPS HAVING TWO GENERATORS

By

Butrus Basmaji

Submitted in Partial Fulfillment for the Requirements
of the Degree Master of Science
in the Mathematics Department of the
American University of Beirut
Beirut, Lebanon,
1964

GROUPS HAVING TWO GENERATORS

Butrus Basmaji

AKNOWLEDGEMENT

The writer wishes to express his deepest gratitude to Professor Peter Yff, whose encouragement and most valuable advice and guidance during the years 1963, 1964 made this work possible.

He is also indebted to Miss Mona Jabbour for her patience and skill in typing the manuscript.

ABSTRACT

This paper is a treatment of groups having two generators, one of which generates a normal subgroup. The emphasis is on finding all the distinct groups satisfying certain relations. Remarks are added to provide a deeper insight of the theory. The illustrative examples, however, are chosen to clarify it and indicate many of the possible applications.

The first chapter contains a section on the isomorphism of finite groups. This forms the basis on which the properties of the groups in the second chapter depend. A result in number theory is proved to help the study of p-groups and other special groups.

Remarks on infinite groups are added in the third chapter. The definitions used here conform to those of the finite case.

TABLE OF CONTENTS

CHAPTER I

THE GROUP G(n,m,r)

1. Introduction

In this chapter finite groups of two generators will be studied. To treat them in their general forms is beyond the scope of this paper. However, some properties of the groups, in which one of the generators generates a normal subgroup, will be studied.

Let the group G (if it exists) be genrated by the elements a and b of orders n and m respectively, satisfying the following relations,

$$a^n = b^m = e, \quad a^k = b^h$$
$$ba = a^r b \qquad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

where none of the integers, (n,k) and (m,h) are one. Let $k|n$ and $h|m$ (In ssection 6 this additional relation will be shown to be redundent.) then k and h are the smallest positive integers such that the above relation holds. The set

$$G(n,m,r) = \left\{ a^i b^j : i = 0,1,\ldots, n-1,\ j = 0,1,\ldots,h-1 \right\} \quad \ldots\ldots (2)$$

Contains every element of G. The element a^k is of order $\frac{n}{k}$ and b^h is of order $\frac{m}{h}$.

But since $a^k = b^h$, it follows that

$$\frac{n}{k} = \frac{m}{h} \quad \text{or} \quad hn = km.$$

Also

$$a^k b = b^h b = bb^h = ba^k = a^{kr} b,$$

which gives

$$a^k = a^{kr} ;$$

and

$$ab^h = aa^k = a^k a = b^h a = a^{r^h} b^h,$$

which gives

$$a = a^{r^h} .$$

These imply that

$$kr \equiv k \bmod n$$
$$r^h \equiv 1 \bmod n \qquad \text{.....(3)}$$

THEOREM 1. A necessary and sufficient condition for the set G(n,m,r) to be a group is that r satisfy relations (3). Also G(n,m,r) is of order hn = km.

PROOF: Let r satisfy relations (3) to prove that G(n,m,r) satisfies the axioms of a group [1, p.2].

1. If $a^x b^y$ and $a^z b^w$ are in G(n,m,r) then

$$a^x b^y a^z b^w = a^{x+zr^y} b^{y+w} = a^{x+zr^y+lk} b^s$$

where $0 \leq s < h$ and $y + w = lh + s$

$a^x b^y a^z b^w$ is in G(n,m,r) since $x + zr^y + lk$ can be reduced modulo n and $s < h$.

The elements of G(n,m,r) are unique for suppose

$$a^x b^y = a^z b^w$$

then left-multiply by a^{-z} and right-multiply by b^{-y}

$$a^{x-z} = b^{w-y}$$

this implies that $x - z \equiv 0 \bmod k$ and $w - y \equiv 0 \bmod h$.

But $0 \leq w < h$ and $0 \leq y < h$, so $w - y = 0$ and $w = y$;

therefore

$$b^y = b^w \quad \text{and} \quad a^x = a^z .$$

But again

$$x \equiv z \bmod n$$

and

$$0 \leq x < n, \; 0 \leq z < n$$

and hence

$$z = x.$$

2. The associative law holds, for

$$(a^x b^y a^z b^w) a^s b^t = a^{x+zr^y} b^{y+w} a^s b^t$$

$$= a^{x+zr^y+sr^{y+w}} b^{y+w+t}$$

and

$$a^x b^y (a^z b^w a^s b^t) = a^x b^y a^{z+sr^w} b^{w+t}$$

$$= a^{x+r^y(z+sr^w)} b^{y+w+t}$$

$$= a^{x+zr^y+sr^{y+w}} b^{y+w+t} .$$

Therefore

$$(a^x b^y a^z b^w) a^s b^t = a^x b^y (a^z b^w a^s b^t).$$

3. e is the identity element of G(n,m,r) for

$$e(a^x b^y) = (ea^x)b^y = a^x b^y,$$

since e is defined as identity element of $\{a\}$.

Similarly
$$(a^x b^y)e = a^x(b^y e) = a^x b^y .$$

4. The inverse of $a^x b^y$ exists in G(n,m,r).

If y = 0 then a^{-x} is in G(n,m,r). Let y > 0 then

$$(a^x b^y)^{-1} = b^{-y} a^{-x} = b^{m-y} a^{n-x}$$

$$= a^{(n-x)r^{m-y}} b^{m-y},$$

in which the exponents can be reduced by the given relations. Hence $(a^x b^y)^{-1}$ is in G(n,m,r). In fact

$$a^x b^y a^{(n-x)r^{m-y}} b^{m-y}$$

$$= a^x a^{(n-x)r^{m-y}r^y} b^y b^{m-y}$$

$$= a^{x+(n-x)r^m} .$$

Since $r^h \equiv 1 \bmod n$ implies that $r^m \equiv 1 \bmod n$ the above expression reduces to

$$a^{x+n-x} = a^n = e.$$

Similarly
$$a^{(n-x)r^{m-y}} b^{m-y} a^x b^y = e.$$

Therefore G(n,m,r) is a group of order km = hn.

Since the necessity of (3) was proved above, the proof is now complete.

From this point onwards G(n,m,r) will always denote the group.

2. Normal Subgroups of G(n,m,r).

The familiar normal subgroups, namely the center Z and the commutator group C will be studied here [1, p.103]. In section four some characteristic subgroups will be studied. We will denote

$$D = \{a\} \cap \{b\} = \{a^k\} = \{b^h\}$$

which is also a normal subgroup and its order is $\frac{n}{k} = \frac{m}{h}$.

Let us find the center Z of G(n,m,r). Suppose $a^x b^y$ is in Z. Then $a^x b^y$ commutes with every element of G(n,m,r);

i.e., $a^z b^w a^x b^y b^{-w} a^{-z} = a^x b^y$ for any z and w.

This implies

$$a^{z+xr^w-zr^y} b^y = a^x b^y,$$

which gives

$$z + xr^w - zr^y \equiv x \bmod n .$$

Since z and w are independent then $z + xr^w - zr^y \equiv x \bmod n$ if and only if $r^y \equiv 1 \bmod n$ and $xr \equiv x \bmod n$. The solutions of the first are y = 0, t, ..., where t is the smallest positive integer such that $r^t \equiv 1 \bmod n$, and the solutions of the second are $x = 0, \frac{n}{(r-1,n)}, \ldots$

Therefore

$$Z = \left\{ a^{\frac{n}{(r-1,n)}}, b^t \right\}$$

and since $t \mid h$ and $\frac{n}{(r-1,n)} \mid k$, the order of Z is $\frac{h}{t}(r-1,n)$.

To find the commutator subgroup C, we begin by

computing a general commutator. Let $a^x b^y$, $a^z b^w$ be any two elements of G(n,m,r). Then

$$a^x b^y a^z b^w b^{-y} a^{-x} b^{-w} a^{-z}$$

$$= a^{x+zr^y} a^{-xr^w-z}$$

$$= a^{x(1-r^w)-z(1-r^y)}$$

$$= a^{f(1-r)}$$

where
$$f = x(1 + r + \ldots + r^{w-1}) - z(1 + r + \ldots + r^{y-1}).$$

But
$$aba^{-1} b^{-1} = a^{1-r} .$$

Therefore every commutator is a power of a^{1-r} which implies that C is a cyclic subgroup and

$$C = \left\{ a^{1-r} \right\} = \left\{ a^{r-1} \right\} \quad \text{of order } \frac{n}{(r-1,n)} .$$

A certain interesting case arises when $r \equiv 1 \bmod k$. Then

$$r = sk + 1$$

and
$$a^{-1} ba = a^{r-1} b = a^{sk} b = b^{sh+1} .$$

Hence $\left\{ b \right\}$ is normal in G(n,m,r). Although both of the generators of this case generate normal subgroups the elements

$$a^{-1}(a^x b^y)a = a^{-1+x+r^y} b^y$$

and
$$b(a^x b^y)b^{-1} = a^{xr} b^y$$

might not be powers of $a^x b^y$ for any x and y. Therefore $\{a^x b^y\}$ need not be normal. This will be illustrated in the following examples.

1. The group G(4,4,3) where k = h = 2, usually written as G(4,4,-1), is known as the quaternion group. Every subgroup is normal is this group.

2. G(9,27,4) having the defining relations,

$$a^9 = b^{27} = e\ , \quad a^3 = b^9\ , \quad ba = a^4 b,$$

is a non-Abelian p-group in which $\{a\}$ and $\{b\}$ are normal. The subgroup $\{ab^6\}$ is not normal in G(9,27,4) since

$$bab^6\ b^{-1} = a^4\ b^6,$$

and $\{ab^6\}$ is of order three having the elements

$$e,\ ab^6,\ a^5\ b^3.$$

However since $\{ab^6\} \cap \{b\} = \{e\}$

and $\{ab^6,\ b\} = \{a,b\} = G(9,27,4)$

by putting $c = b^{19}$ and $d = ab^6$ we have

$$c^{27} = d^3 = e \qquad dc = c^{-8}\ d,$$

Hence the above are defining relations of G(9,27,4). We will see later that this will be denoted by S(27,3,-8).

3. Factor Groups

Here we will find out that all the non-cyclic factor

groups, [1, p.102], of the normal subgroups in section two are isomorphic to $G(n',m',r')$ for some n', m', and r'.

Let us first find the factor group with respect to D. Since $D = \{a^k\} = \{b^h\}$

$G(n,m,r)/D$ consists of the cosets

$$D,\ Da,\ \ldots,\ Da^{k-1},$$

$$Db, Dab, \ldots, Da^{k-1}b,$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$Db^{h-1}, Dab^{h-1}, \ldots, Da^{k-1}b^{h-1},$$

and

$$(Db)(Da) = D\,ba = Da^r b$$

$$= Da^{r'} b \text{ where } 0 < r' < k,\ r' \equiv r \bmod k$$

$$= (Da)^{r'} (Db)$$

and

$$(Da)^k = (Db)^h = D$$

therefore

$$G(n,m,r)/D \cong G(k,h,r') \text{ where } r' \equiv r \bmod k$$

It will be easily noticed that in $G(k,h,r')$ the first relation of (1) implies the second. Such groups will be studied in the second chapter and will be denoted by $S(n,m,r)$. However an interesting relation between $G(n,m,r)$ and $S(n,m,r)$ will be studied at the end of this section.

Using the new notation we write

$$G(n,m,r)/D \cong S(k,h,r'),\ r' \equiv r \bmod k$$

which is of order kh.

To find the factor group with respect to the center Z we take $Z = \{a^{\frac{n}{(r-1,n)}}, b^t\}$ where t is the smallest positive power such that $r^t \equiv 1 \bmod n$.

It is easy to see that $t|h$ and $\frac{n}{(r-1,\ n)} | k$.

Let

$$\frac{n}{(r-1,\ n)} = n'$$

then

$G(n,m,r)/Z$ consists of the cosets

$$Z,\ Za,\ \ldots,\ Za^{n'-1}$$

$$Zb, Zab, \ldots, Za^{n'-1}\ b,$$

$$\vdots \qquad\qquad \vdots$$

$$Zb^{t-1}, Za\ b^{t-1}, \ldots, Za^{n'-1}\ b^{t-1},$$

in which

$$(Za)^{n'} = (Zb)^t = Z$$

and

$$(Zb)(Za) = Zba = Za^r\ b$$

$$= Za^{r'}\ b \qquad (0 \leq r' < n',\ r' \equiv r \bmod n')$$

$$= (Za)^{r'}\ (Zb)$$

therefore

$$G(n,m,r)/Z \cong S(n',t,r')$$

and is of order

$$n't = \frac{tn}{(r - 1,\ n)}.$$

For the factor group with respect to the commutator

subgroup C we know that $C = \{a^{r-1}\}$ and therefore we have $G(n,m,r)/C$ consisting of

$$C,\ Ca,\ \ldots\ldots,\ Ca^{(r-1,n)-1}$$

$$Cb, Cab, \ldots\ldots, Ca^{(r-1,n)-1}b$$

$$\vdots \qquad\qquad \vdots$$

$$Cb^{h-1}, Cab^{h-1}, \ldots, Ca^{(r-1,n)-1}b^{h-1}$$

where

$$Ca^k = Cb^h.$$

In the cyclic group $\{Ca\}$, $\{Ca^k\}$ is a cyclic subgroup of order $\frac{(r-1,n)}{(r-1,k)}$ and $\{Ca^k\} = \{Ca^{(r-1,k)}\}$. Hence Cb^h is of the same order as $Ca^{(r-1,k)}$. If we let

$$s = (r-1,n) \text{ and } q = h\,\frac{(r-1,n)}{(r-1,k)}$$

then

$$(Ca)^s = (Cb)^q = C,\ (Ca)^k = (Cb)^h,\ (Cb)(Ca) = (Ca)(Cb).$$

Here k does not in general divide s. However it will be seen in section 6 that $(s,k) = (r-1,k)$ may be replaced for k. Therefore $G(n,m,r)/C$ is of order $hs = h(r-1,n)$ and is isomorphic to $G(s,q,1)$ with the defining relations

$$a^s = b^q = e,\quad a^{(s,k)} = b^h,\quad ba = ab.$$

If the defining relations of $S(n,m,r)$ of order nm are,

$$a^n = b^m = e,\quad ba = a^r b.$$

then by theorem 1 $S(n,m,r)$ is a group if and only if

$$r^m \equiv 1 \bmod n .$$

If integers h and k exist such that $\frac{n}{k} = \frac{m}{h}$, $kr \equiv k \bmod n$, and $r^h \equiv 1 \bmod n$ then $K = \{ a^k b^{-h} \}$ is normal in $S(n,m,r)$. In fact K is included in the center Z.

$S(n,m,r)/K$ consists of the cosets

$$K, Ka, \ldots, Ka^{n-1}$$

$$Kb, Kab, \ldots, Ka^{n-1} b$$

$$\vdots \quad \vdots \qquad \vdots$$

$$Kb^{h-1}, Kab^{h-1}, \ldots, Ka^{n-1} b^{h-1}$$

Here

$$(Ka)^n = (Kb)^m = K$$

and

$$(Ka)^k = (Kb)^h$$

since

$$a^k b^{-h} \text{ is in } K.$$

Also

$$(Kb)(Ka) = Kba = Ka^r b = (Ka)^r (Kb).$$

Therefore

$$S(n,m,r)/K \cong G(n,m,r).$$

4. Nilpotent Groups.

The groups $G(n,m,r)$ need not be nilpotent [2, p.149]. In fact there exists a necessary and sufficient condition that makes this true. In this section this will be proved and its class will be found.

Consider a lower central series [2,p. 150] of $G(n,m,r)$,

i.e.,

$$G(n,m,r) = \Gamma_0[G(n,m,r)] \supseteq \Gamma_1[G(n,m,r)] \supseteq \ldots \supseteq \Gamma_s[G(n,m,r)] \supseteq \ldots$$

Here
$$C = \Gamma_1[G(n,m,r)] = \{ a^{r-1} \} = \{ a^{1-r} \}$$

and
$$\Gamma_2[G(n,m,r)] = \{ (C, a^z b^w) \} \text{ for all } z \text{ and } w$$

$$= \{ (a^{(1-r)f}, a^z b^w) \} \text{ for all } f$$

$$= \{ a^{(1-r)f} a^z b^w a^{(r-1)f} b^{-w} a^{-z} \}$$

$$= \{ a^{(1-r)f+(r-1)fr^w} \}$$

$$= \{ a^{(1-r)^2} \} \text{ (take } f = w = 1\text{)}$$

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

By induction it can be proved that

$$\Gamma_s[G(n,m,r)] = \{ a^{(r-1)^s} \} \quad \text{for any positive } s.$$

$G(n,m,r)$ is nilpotent if for all $s \geq g$, where g is a positive finite integer, $\Gamma_s[G(n,m,r)] = \{ e \}$. But the lower central series now can be written as

$$G(n,m,r) \supseteq \{ a^{r-1} \} \supseteq \{ a^{(r-1)^2} \} \supseteq \ldots \supseteq \{ a^{(r-1)^s} \} \supseteq \ldots$$

Suppose there exists an s such that

$$\Gamma_s[G(n,m,r)] = \{ a^{(r-1)^s} \} = \{ e \}$$

then $(r-1)^s \equiv 0 \bmod n$ which implies that

$$n \mid (r-1)^s \quad \text{or} \quad (r-1)^s = ln \quad \text{where } l \text{ is an integer.}$$

This implies that if p is a prime dividing n then p should also divide r-1, but the inverse need not be true. However if $p \mid n$ and $p \nmid r-1$ then $p \nmid (r-1)^s$ for any finite s and $(r-1)^s \not\equiv 0 \bmod n$ which implies that

$$\{ a^{(r-1)^s} \} \neq \{ e \} \qquad \text{for any finite } s,$$

this proves,

THEOREM 2. A necessary and sufficient condition for $G(n,m,r)$ to be nilpotent is that

$$r \equiv 1 \bmod p \quad \text{for every prime } p \text{ dividing } n.$$

If $G(n,m,r)$ is nilpotent we can also calculate its class, i.e. the smallest positive integer s such that $\{ a^{(r-1)^s} \} = \{e$

For this purpose let

$$n = p_1^{n_1} \cdots p_t^{n_t}, \quad \text{and} \quad r - 1 = xp_1^{e_1} \cdots p_t^{e_t}$$

where p_i is a prime, $n_i > 0$, $e_i > 0$ and $(x,p_i) = 1$ for $i = 1, \ldots, t$ and $(p_i,p_j) = 1$ if $i \neq j$

Let $[n_i/e_i]$ denote the largest integer which is less than or equal to n_i/e_i and let

$$g = \operatorname{Max}_i(-[-n_i/e_i]).$$

Note that $-[-n_i/e_i]$ is the smallest integer which is greater than or equal to n_i/e_i, [3, p.78]. Therefore

$$ge_i - n_i \geq e_i \frac{n_i}{e_i} - n_i \qquad \left(\text{since } g \geq \frac{n_i}{e_i}\right)$$

$$\geq 0$$

Hence for

$$i = 1, \ldots, t$$

$$p_i^{n_i} \mid (p_i^{e_i})^g$$

and there exists at least one j such that

$$p_j^{n_j} \nmid (p_j^{e_j})^{g-1}$$

Therefore s = g and G(n,m,r) is nilpotent of class

$$g = \max_i(-[-n_i/e_i]).$$

Note that if $n_1 = n_2 = \ldots = n_t = 1$, then using theorem 2 $r \equiv 1 \bmod p_i$ for i = 1, ..., t. This is true if and only if $r \equiv 1 \bmod p_1 \ldots p_t$, i.e., $r \equiv 1 \bmod n$. Hence in this case there exists no non-Abelian nilpotent group G(n,m,r).

5. The Group R

Even when we fix n and m we might have more than one r such that G(n,m,r) is a group. Let R denote the set of all r's which are incongruent modulo n. This set is finite since the incongruent integers modulo n are finite. Also since $r^h \equiv 1 \bmod n$ then $r^h - 1 = fn$, f an integer and

$$r^h - fn = (r^{h-1})\, r + (-f)n = 1$$

which implies that (r,n) = 1.

However r also satisfies $kr \equiv k \bmod n$.

Suppose r_1 and r_2 are in the set R and since they

commute we have

$$(r_1 r_2)^h \equiv r_1^h r_2^h \mod n$$

$$\equiv r_1^h \cdot 1 \equiv 1.1 \equiv 1 \mod n$$

and

$$(kr_1)r_2 \equiv kr_2 \equiv k \mod n .$$

Therefore $r_1 r_2$ is in R.

1 is in R since $1^h \equiv 1$ and $1.k \equiv k \mod n$.

For every r in R there exists a $t|h$ which is the smallest positive integer such that $r^t \equiv 1 \mod n$. Since r is in R, r^{t-1} is in R and $(r)(r^{t-1}) \equiv 1 \mod n$.

The elements of the set R are associative and commutative since they are integers modulo n.

This proves that the set R under the congruence relation forms a group. We call this group as the group R. To avoid confusion, the period of an element of R will mean its order. Order will be used for elements of abstract groups.

6. Isomorphisms of the Groups G(n,m,r)

The number of distinct non-isomorphic groups G(n,m,r) does not depend on the order of the group R but on the number of cyclic subgroups that R contains. Even if $r \not\equiv r_2 \mod n$ the groups $G(n,m,r_1)$ and $G(n,m,r_2)$ may be isomorphic to each other. A theorem in number theory, due to Dirichlet has been applied to prove theorem 3, [5, p. 217]. It states:

If $(z,t) = 1$, then there are infinitely many primes of the form $z + ft$.

Using this we prove

THEOREM 3. $G(n,m,r_1) \cong G(n,m,r_2)$ if $\{r_1\} = \{r_2\}$.

PROOF: Since r_1 and r_2 generate the same subgroup they have the same period and r_2 is a power of r_1.

Let t be the period of r_1 and let

$G(n,m,r_1) = \{a,b\}$ with $a^n = b^m = e$, $a^k = b^h$, $ba = a^{r_1} b$

and

$G(n,m,r_2) = \{c,d\}$ with $c^n = d^m = e$, $c^k = d^h$, $dc = c^{r_2} d$

here

$$r_2 \equiv r_1^z \bmod n \quad \text{where} \quad (z,t) = 1.$$

Suppose $G(n,m,r_1) \cong G(n,m,r_2)$ and the isomorphism is given by

$$(c,d) \to (a^x, b^y).$$

This implies that

$$(x,n) = 1, \ (y,m) = 1 \quad \ldots\ldots\ldots\ldots (i)$$

also

$$c^k = d^h \to a^{xk} = b^{yh}$$

therefore

$$b^{xh} = b^{yh}, \ a^{xk} = a^{yk}$$

and

$$h(x-y) \equiv 0 \bmod m \text{ or } x \equiv y \bmod \frac{m}{h}$$

$$k(x-y) \equiv 0 \bmod n \text{ or } x \equiv y \bmod \frac{n}{k} \qquad \ldots\ldots\ldots (ii)$$

However since $\frac{m}{h} = \frac{n}{k}$ the two relations of (ii) are equivalent.

Also $$dc = c^{r_2} d \rightarrow b^y a^x = a^{xr_1^y} b^y$$

$$c^{r_2} d \rightarrow a^{xr_2} b^y$$

$$xr_2 \equiv xr_1^y \bmod n$$

$$r_2 \equiv r_1^y \bmod n \quad \text{since } (x,n) = 1$$

But

$$r_2 \equiv r_1^z \bmod n$$

Hence

$$r_1^z \equiv r_1^y \bmod n$$

and

$$z \equiv y \bmod t \quad \ldots\ldots\ldots\ldots \text{(iii)}$$

This isomorphism is true if we can prove that integers x and y exist satisfying the relations (i), (ii), and (iii) where z is given.

From (iii)

$$t \mid y - z \quad \text{or} \quad ft = y - z$$

and $y = z + ft$ where $(t,z) = 1$.

In the set $\{ z + t, z + 2t, \ldots, z + ft, \ldots \}$, by Dirichlet's theorem, there exist infinitely many primes, and since only a finite number of primes divide m then there exists a prime y_p in this set such that $y_p \nmid m$ or $(y_p, m) = 1$.

From (ii)

$$x \equiv y_p \bmod \frac{m}{h}$$

or $\frac{m}{h} \mid x - y_p$ or $x - y_p = f' \frac{m}{h}$, f' an integer

and $x = y_p + f' \frac{m}{h}$ where $(y_p, \frac{m}{h}) = 1$ since $(y_p, m) = 1$.

Again in the set $\left\{ y_p + \frac{m}{h}, \ldots, y_p + f' \frac{m}{h}, \ldots \right\}$, by Dirichlet's theorem, there exist infinitely many primes and since only a finite number of primes divide n there exists a prime x_p in this set such that $x_p \nmid n$ or $(x_p, n) = 1$.

Therefore the integers, x_p and y_p, satisfy relations (i), (ii) and (iii) which completes the proof.

With the help of this theorem we can state that the number of distinct non-isomorphic groups G(n,m,r) is less than or equal to the number of cyclic subgroups that R contains.

This theorem also can be applied to get an interesting result in number theory.

$$G(n,m,r) \cong G(n,m,r^f) \text{ if } (f,t) = 1$$

where t is the period of r. This implies that the commutator subgroup of order $\frac{n}{(r-1,\ n)}$ of G(n,m,r) has the same order as the commutator subgroup of order $\frac{n}{(r^f-1,n)}$ of $G(n,m,r^f)$. Hence

$$\frac{n}{(r-1,\ n)} = \frac{n}{(r^f-1,n)}$$

and we have

$$(r-1,\ n) = (r^f-1,\ n).$$

Therefore we have proved,

COROLLARY. If $r^t \equiv 1 \bmod n$ and if $(f,t) = 1$ then

$$(r-1,n) = (r^f-1,n).$$

This is true for any r relatively prime to n and any f such that $(f,t) = 1$ since we can define a group whose group R is the set of all integers relatively prime to n. In fact this group is

$$S(n, \phi(n), r)$$

where ϕ is Euler's function [3, p.23].

Now let us prove a theorem which, with theorem 3, will be very important to find the properties of the groups in chapter 2.

THEOREM 4. $G(n,m,r_1) \cong G(n,m,r_2)$ implies

1. $(r_1-1,n) = (r_2-1,n)$ and period of r_1 = period of r_2
2. $\{r_1\} = \{r_2\}$ if $(k,h) = 1$ or $(r_i-1,h) = 1$ for $i = 1$ or 2.

PROOF: 1. Suppose $(r_1-1,n) \neq (r_2-1,n)$. Then the commutator subgroups of $G(n,m,r_1)$ and $G(n,m,r_2)$ would be of orders $\frac{n}{(r_1-1, n)}$ and $\frac{n}{(r_2-1,n)}$ respectively, which are not equal. But since the commutator groups are characteristic [2, p.150], this would imply that $G(n,m,r_1) \ncong G(n,m,r_2)$. Hence we have a contradiction.

On the other hand suppose that the period of r_i is t_i for $i = 1,2$ respectively and suppose $t_1 \neq t_2$. Then the centers of $G(n,m,r_1)$ and $G(n,m,r_2)$ would be of orders $\frac{h}{t_1}(r_1-1,n)$ and $\frac{h}{t_2}(r_2-1,n)$ which are unequal

since $(r_1-1,n) = (r_2-1,n)$. But the centers are also characteristic subgroups [2, p.31], which would imply that $G(n,m,r_1) \ncong G(n,m,r_2)$. Hence we get a contradiction.

2. Let $G(n,m,r_1) = \{a,b\}$ and $G(n,m,r_2) = \{c,d\}$ and let the isomorphism be given by

$$(c,d) \to (a^x b^y,\ a^z b^w)$$

From this we get

$$dc = c^{r_2} d \to a^z b^w a^x b^y = a^{z+r_1^w} b^{w+y}$$

$$c^{r_2} d \to a^{x(1+r_1^y+\ldots+r_1^{(r_2-1)y})+zr_1^{r_2y}} b^{r_2y+w}$$

and

$$c^k = d^h \to a^{x(1+r_1^y+\ldots+r_1^{(k-1)y})} b^{ky}$$

$$d^h \to a^{z(1+r_1^w+\ldots+r_1^{(h-1)w})} b^{hw} = a^f$$

and these give

$$w + y \equiv r_2 y + w \bmod h$$

or

$$(r_2-1)y \equiv 0 \bmod h$$

and

$$ky \equiv 0 \bmod h$$

If $(r_2-1,h) = 1$ or $(k,h) = 1$ then $y = 0$

and

$$(c,d) \to (a^x,\ a^z b^w)$$

Hence

$$(x,n) = 1,\ (w,h) = 1 \text{ or } (w,t) = 1 \ (t \text{ period of } r_i)$$

and

$$dc = c^{r_2} d \to a^z b^w a^x = a^{z+xr_1^w} d^w$$

$$c^{r_2} d \to a^{xr_2+z} d^w$$

Hence

$$r_2 \equiv r_1^w \bmod n$$

and since r_1 and r_2 by part 1, have the same period we have

$$\{r_1\} = \{r_2\}.$$

If $(r_1-1,h) = 1$ we would come to the same result by taking

$$(a,b) \rightarrow (c^x d^y, c^z d^w).$$

For every pair of integers k and h such that $\frac{n}{k} = \frac{m}{h}$ there exists at least one group G(n,m,r). However k depends on h and can be made larger by making m smaller. This will be given by

THEOREM 5. If g is a positive integer dividing m such that $(h, \frac{m}{g}) = 1$ then the group G(n,m,r) with the defining relations,

$$a^n = b^m = e, \quad a^k = b^h, \quad ba = a^r b,$$

is isomorphic to the group G(n,g,r) with the defining relations,

$$c^n = d^g = e', \quad \left(c^{m/g}\right)^k = d^h, \quad dc = c^r d.$$

PROOF: It is clear that $h|g$ and $\frac{m}{g}|n$. Let $b_1 = b^{m/g}$. Since $(h, \frac{m}{g}) = 1$ there exist integers x and y such that $xh + y\frac{m}{g} = 1$. Hence

$$a^{xk} b_1^y = a^{xk}\left(b^{m/g}\right)^y = b^{xh+(m/g)y} = b.$$

Therefore

$$G(n,m,r) = \{a,b\} = \{a,b_1\}.$$

b_1^s is not an element of $\{a\}$ if $h \nmid s$, for suppose it is: then it implies that $b^{m/g\ s}$ is an element of a. From the defining relations of $G(n,m,r)$ we see that $h \mid \frac{m}{g} s$. But $h \nmid \frac{m}{g}$ hence $h \mid s$, a contradiction. Hence only the h distinct powers of b_1 are elements of $\{a\}$ $b_1^h = b^{m/g\ h} = a^{m/g\ k}$ and $b_1^g = e$.

Since $\frac{m}{g} \mid \frac{m}{h}$ then $\frac{m}{g} k \mid \frac{m}{h} k = n$.

We check that $n/\frac{m}{g} k = \frac{n}{k}/\frac{m}{g} = \frac{m}{h}/\frac{m}{g} = g/h$.

Therefore the defining relations of $G(n,m,r)$ can be written in terms of a and b_1 and these are

$$a^m = b_1^g = e,\ \left(a^{m/g}\right)^k = b_1^h,\ b_1 a = a^{r^{m/g}} b_1 .$$

These are the defining relations of $G(n,g,r^{m/g})$. Since $(\frac{m}{g}, h) = 1$ then $(\frac{m}{g}, t) = 1$ where t is the period of r. Hence $\{r\} = \{r^{m/g}\}$ and by applying theorem 3 we have

$$G(n,g,r) \cong G(n,g,r^{m/g})$$

and therefore

$$G(n,m,r) \cong G(n,g,r).$$

All the integers g dividing m such that $(h, \frac{m}{g}) = 1$ form a set. m is an element of this set. If m is the only element in this set then $G(n,m,r)$ can not be reduced by this method, However, if h is an element of this set then it is the smallest and we can state

COROLLARY. If $(h, \frac{m}{h}) = 1$ then the group $G(n,m,r)$ as defined

in theorem 6 is isomorphic to S(n,h,r) which has the defining relations,

$$c^n = d^h = e' \ , \ dc = c^r d.$$

Now let us show that the relation, k | n and h | m, added in section 1 is redundant by proving an isomorphism between G = $\{a,b\}$ with the defining relations,

$$a^n = b^m = e, \quad a^f = b^s, \quad \text{and} \quad ba = a^r b$$

and G(n,m,r) where $k = (f,n)$ and $h = (s,n)$.
First we study G and reduce f to k. Here r should satisfy the congruence relation

$$r^s \equiv r^m \equiv 1 \bmod n \quad \text{and} \quad fr \equiv f \bmod n.$$

Since there exist integers z and w such that $zs + wm = h$, then the above first relation is satisfied if and only if

$$r^h \equiv 1 \bmod n.$$

Also by dividing the second relation by f we get

$$r \equiv 1 \bmod \frac{n}{(f,n)} \quad \text{which equivalen to } kr \equiv k \bmod n,$$

since

$$k = (f,n).$$

Since a^k and b^s generate the same cyclic group,

$$a^k = b^g \ , \ s \mid g, \text{ but } \{a^k\} = \{a^f\} = \{b^g\} = \{b^s\} = \{b^h\}.$$

Hence

$$(g,m) = (s,m) = h.$$

Therefore the defining relations of G can be written as

$$a^n = b^m = e, \quad a^k = b^g, \quad \text{and} \quad ba = a^r b.$$

We now construct an isomorphism between G and $G(n,m,r) = \{c,d\}$.

Suppose the isomorphism $G \cong G(n,m,r)$ is given by

$$(a,b) \to (c^x, d^y).$$

This implies that

$$(x,n) = (y,m) = 1 \quad \ldots\ldots\ldots\ldots (i)$$

Also

$$ba = a^r b \to d^y c^x = c^{xr^y} d^y$$

$$a^r b \to c^{xr} d^y.$$

Therefore

$$xr \equiv xr^y \bmod n$$

or

$$y \equiv 1 \bmod t \quad \ldots\ldots\ldots\ldots\ldots (ii)$$

where t is the period of r.

Moreover

$$a^k = b^g \to c^{xk} = d^{yg} = d^{xh}$$

hence

$$xh \equiv yg \bmod m. \quad \ldots\ldots\ldots\ldots (iii)$$

The isomorphism holds if x and y exist satisfying relations (i), (ii) and (iii).

From (ii) it is seen that $y_p = 1$ satisfies (i) and (ii).

(iii) can be written as

$$x \equiv \frac{g}{h} \bmod \frac{m}{h}.$$

But $(g,m) = h$ implies that $(g/h, m/h) = 1$ and therefore by Dirichlet's theorem in the set $\left\{ \frac{g}{h} \; , \; \frac{g}{h} + \frac{m}{h}, \ldots, \frac{g}{h} + z\frac{m}{h}, \ldots \right\}$ there exist infinitely many primes. Pick $x_p \nmid n$ or $(x_p, n) = 1$. Hence x_p exists satisfying (ii) and (i) .

Therefore integers x and y exist for which the isomorphism holds.

By this result we can say that taking $k \mid n$ and $h \mid m$ did not make our treatment of the group G(n,m,r) less general.

7. An Illustrative Example.

Suppose we want to find all the groups S(77,70,r) with the defining relations,

$$a^{77} = b^{70} = e, \quad ba = a^r b.$$

r should satisfy the congruence relation $r^{70} \equiv 1 \bmod 77$. The group R is the direct product of $\{8\}$ of order 10 and $\{-1\}$ of order 2, i.e. it is of order 20. The cyclic subgroups of R are generated by ± 1, ± 8, ± 15, ± 43 since R has the elements

$$\pm 1, \pm 8, \pm 8^2 = \pm 64, \pm 8^3 = \pm 50, \pm 8^4 = \pm 15, \pm 8^5 = \pm 43,$$

$$\pm 8^6 = \pm 36, \pm 8^7 = \pm 57, \pm 8^8 = \pm 71, \text{ and } \pm 8^9 = \pm 29.$$

Hence by applying theorems 3 and 4 we have only eight distinct non-isomorphic groups. These are

1. $S(77,70,1)$ $Z = \{ a,b \}$, $C = \{ e \}$
2. $S(77,70,8)$ $Z = \{ a^{11}, b^{10} \}$, $C = \{ a^7 \}$
3. $S(77,70,15)$ $Z = \{ a^{11}, b^5 \}$, $C = \{ a^7 \}$
4. $S(77,70,43)$ $Z = \{ a^{11}, b^2 \}$, $C = \{ a^7 \}$
5. $S(77,70,-1)$ $Z = \{ b^2 \}$, $C = \{ a \}$
6. $S(77,70,-8)$ $Z = \{ b^{10} \}$, $C = \{ a \}$
7. $S(77,70,-15)$ $Z = \{ b^{10} \}$, $C = \{ a \}$
8. $S(77,70,-43)$ $Z = \{ a^7, b^2 \}$, $C = \{ a^{11} \}$

Note that $S(77,70,-8)$ and $S(77,70,-15)$ are not isomorphic by the second part of theorem 4, i.e., since $\{-8\} \neq \{-15\}$ and $(-8\ -1,\ 70) = 1$.

For any r, from the group R, $S(77,70,r)$ is isomorphic to one of the groups listed above. For instance $S(77,70,8) = \{ a,b \}$ and $S(77,70,57) = \{ c,d \}$ are isomorphic. Since $8^7 \equiv 57 \bmod 77$, by using the proof of theorem 3 we find that this isomorphism may be given by

$$(c,d) \rightarrow (a^x, b^y)$$

where $(x,77) = 1$ and y is a member of the set 17,27,37,47,67,57. Hence there exist $6\phi(77) = 360$ pairs of integers x and y for which the above isomorphism is satisfied.

The cyclic subgroup $K = \{ a^{22}\ b^{30} \}$ has the elements $e,\ a^{22}\ b^{30},\ a^{44}\ b^{60},\ a^{66}\ b^{20},\ a^{11}\ b^{50},\ a^{33}\ b^{10},\ a^{55}\ b^{40}$. K is included in the center Z of the first four groups listed above, and hence is normal in them. But

$$ba^{22}\, b^{30}\, b^{-1} = a^{22r}\, b^{30}$$

is not an element of K for r = -1, -8, -15 and -43, for if it had been then

$$22r \equiv 22 \bmod 77$$

or

$$r \equiv 1 \bmod 7$$

which is not true. However, it is true for r = 1,8,15 and 43. S(77,70,r)/K will have the defining relations

$$(Ka)^{77} = (Kb)^{70} = K$$

$$(Ka)^{22} = (Kb)^{40} \text{ since } a^{22}b^{-40} = a^{22}b^{30} \text{ is in K.}$$

$$(Kb)(Ka) = Kba = Ka^{r}\, b = (Ka)^{r}(Kb).$$

Hence it has the defining relations

$$c^{77} = d^{70} = e' , \quad c^{22} = d^{40} , \quad dc = c^{r}\, d.$$

$$(c^{22})^4 = c^{11} = (d^{40})^4 = (d^{160}) = d^{20}.$$

We check that

$$(40,70) = (20,70) = 10.$$

Therefore, by following the discussion of section 6, the isomorphism of the above group with $G(77,70,r) = \{c',d'\}$ may be given by

$$(c,d) \rightarrow (c'^{x},d')$$

where x = 2,9,16,23,30,37,51,58,65,72. Hence there are at least 10 different ways for the above isomorphism to be satisfied.

Hence there are only four non-isomorphic groups G(77,70,r) with the defining relations,

$$a^{77} = b^{70} = e \ , \quad a^{11} = b^{10} \ , \quad ba = a^r b.$$

These are

1. G(77,70,1) $\quad Z = \{ a,b \}, \quad C = \{ e \}$
2. G(77,70,8) $\quad Z = \{ a^{11} \}, \quad C = \{ a^7 \}$
3. G(77,70,15) $\quad Z = \{ b^5 \}, \quad C = \{ a^7 \}$
4. G(77,70,43) $\quad Z = \{ b^2 \}, \quad C = \{ a^7 \}.$

These could also have been found by solving

$$r^{10} \equiv 1 \bmod 77 \quad \text{and} \quad 11r \equiv 11 \bmod 77.$$

The group R would be the cyclic group $\{8\}$ of order 10. Again isomorphisms between $G(77,70,8) = \{a,b\}$ and $G(77,70,57) = \{c,d\}$ can be constructed. In fact

$$(c,d) \rightarrow (a^x, b^{17})$$

where x is one of the following integers

$$3,10,17,24,31,38,45,52,59,73.$$

We notice that $(10, \frac{70}{10}) = 1$. Hence applying theorem 5 and its corollary we conclude that $G(77,70,r) = \{a,b\}$ and $S(77,10,r) = \{c,d\}$ are isomorphic. This is given by

$$(c,d) \to (a, a^{22} b)$$

or

$$(a,b) \to (c, c^{-22} d).$$

Note that there are eight groups S(77,10,r) for the same values of r, given above for S(77,70,r).

CHAPTER II

THE GROUP A(n,m,r)

1. Introduction.

In this chapter we shall be interested to find the properties of the group A(n,m,r) with the defining relations,

$$a^n = b^m = (ab)^m = e \ , \ ba = a^r b.$$

It can be easily seen that r should satisfy the congruence relation,

$$1 + r + r^2 + \ldots + r^{m-1} \equiv 0 \bmod n \ , \ \ldots\ldots\ldots (1)$$

from which we conclude that $(r,n) = 1$.

However, it will be more convenient to introduce the group S(n,m,r) with the defining relations,

$$a^n = b^m = e \ , \ ba = a^r b.$$

From theorem 1 we see that $r^m \equiv 1 \bmod n$ or

$$r^m - 1 \equiv (r-1)(r^{m-1} + r^{m-2} + \ldots + r + 1) \equiv 0 \bmod n \ \ldots (2)$$

Here it is noticed that every r satisfying congruence (1) also satisfies (2), but the converse is not always true.

Therefore to find all the groups A(n,m,r) for fixed n and m we find all the groups S(n,m,r) and from them we select those that satisfy the relations of A(n,m,r).

This can be done also by solving the congruence $r^m \equiv 1 \bmod n$ and picking all the solutions that satisfy the congruence given by (1).

The group R has some applications in A(n,m,r). But the set of all r need not be the group R and might not even generate it. In fact it is a subset of the group R. If no A(n,m,r) exists, then the set of all r is the empty set. This gives a divergence between the groups S(n,m,r) and A(n,m,r), for although at least one group S(n,m,r) exists for any given n and m, there are strict conditions on n and m for the existence of A(n,m,r). If m is odd then by a glance at congruence (1) we see that n should be odd. However, if m is even then at least one r exists for which congruence (1) is satisfied for every n, namely r = -1, and therefore at least one group A(n,m,r) exists. Further discussion on the existence of A(n,m,r) will be done in section 4.

Moreover, suppose r is of period t. Then $t \mid m$ and the congruence (1) can now be written as

$$\frac{m}{t}(r^{t-1} + r^{t-2} + \ldots + r + 1) \equiv 0 \bmod n .$$

Here note that the quantity between the parenthesis is the sum of the elements of the cyclic group $\{ r \}$. Since

$$\{ r \} = \{ r^f \} \quad \text{if} \quad (f,t) = 1,$$

then

$$r^{t-1} + r^{t-2} + \ldots + r + 1 \equiv (r^f)^{t-1} + (r^f)^{t-2} + \ldots + r^f + 1 \bmod n .$$

therefore r^f also satisfies congruence (1) and $A(n,m,r^f)$ also exists. From theorem 3 we see that $A(n,m,r_1) \cong (A(n,m,r_2)$ if $\{r_1\} = \{r_2\}$.

For example, suppose we want to find all the non-isomorphic groups $A(77,70,r)$ with the defining relations,

$$a^{77} = b^{70} = (ab)^{70} = e,\ ba = a^r b \ \ldots\ldots\ldots (i)$$

r should satisfy the congruence relation

$$r^{69} + r^{68} + \ldots + r^2 + r + 1 \equiv 0 \bmod 77 .$$

which holds if and only if r satisfies the following congruences

$$r^{69} + r^{68} + \ldots + r^2 + r + 1 \equiv 0 \bmod 7 \ \ldots\ldots (ii)$$

and

$$r^{69} + r^{68} + \ldots + r^2 + r + 1 \equiv 0 \bmod 11 \ \ldots\ldots (iii)$$

[3, p.38].

From section 7 chapter I we found that there exist exactly eight non-isomorphic groups $S(77,70,r)$. The values of r for these groups are ± 1, ± 8, ± 15, and ± 43. Each r is congruent to $\pm 1 \bmod 7$ and therefore satisfies (ii).

$$(r-1,11) = 1 \text{ for } r = -1, \pm 8, \pm 15, 43$$

and hence dividing the congruence $(r^{70}-1) \equiv 0 \bmod 11$ by the given $r - 1$ will show that these r's satisfy congruence (iii). -43 and 1 are congruent to $1 \bmod 11$ and it is clear from (iii) that 1 does not satisfy it since $70 \not\equiv 0 \bmod 11$.

Hence there are only six non-isomorphic groups A(77,70,r) with the defining relations (i). These are A(77,70,-1), A(77,70,8), A(77,70,-8), A(77,70,15), A(77,70,-15), A(77,70,43). Note that all these groups are non-Abelian. In fact there exists an Abelian group of the form A(n,m,r) if and only if n divides m.

2. p-Groups.

The study of p-groups of two generators will depend on properties of prime power integers. The following will have important applications.

LEMMA 1. The highest power of p (a prime) that divides $(1 + p^k)^{p^n} - 1$ is p^{n+k} where $k \geq 1$ for $p \neq 2$ and $k \geq 2$ for $p = 2$.

PROOF: by expansion

$$(1+p^k)^{p^n} = 1+p^{n+k} + \sum_{t=2}^{p^n} \binom{p^n}{t} p^{tk}.$$

Hence it is sufficient to prove that

$$\binom{p^n}{t} p^{tk} \equiv \frac{p^n}{t}\left[\frac{(p^n-1)(p^n-2)\ldots(p^n-t+1)}{(t-1)\,!}\right]p^{tk} \equiv 0 \bmod p^{k+n+1}$$

for $t \geq 2$. But the quantity in the brackets is equal to $\binom{p^n-1}{t-1}$ which is an integer, say f. Also $\binom{p^n}{t}$ is an integer and therefore any prime different from p dividing t divides f. Suppose p^s is the highest power of p dividing t, then for the proof of the lemma it is sufficient to show that

$$n - s + t\,k \geq k + n + 1 \text{ or } (t-1)k - s - 1 \geq 0.$$

If $p \neq 2$ then $s \leq t - 2$ or $-s \geq -(t-2)$.

Hence

$$(t-1)k - s - 1 \geq (t-1)k - (t-2) - 1$$

$$\geq (t-1)(k-1)$$

$$\geq 0 \text{ since } t \geq 2 \text{ and } k \geq 1.$$

If $p = 2$ then $s \leq t - 1$ or $-s \geq -(t-1)$.

Hence

$$(t-1)k - s - 1 \geq (t-1)k - (t-1) - 1$$

$$\geq t(k-1) - k$$

$$\geq 2k - 2 - k \quad \text{since } t \geq 2$$

$$\geq k - 2 \geq 0 \quad \text{since } k \geq 2.$$

This completes the proof of the lemma.

It is important to notice that the highest power of 2 dividing $(2^k-1)2^n - 1$ is 2^{n+k} for $k \geq 2$.

The integers that are relatively prime to n and less than n form an Abelian group under multiplication modulo n. In some textbooks this group is denoted by M(n) [5, p.207]. $M(p^n)$ is a cyclic group of order $\phi(p^n) = p^{n-1}(p-1)$ when p(a prime) $\neq 2$ [4, p.107] and $M(2^n) = \{5, -1\}$ where 5 is of period 2^{n-2} and -1 is of period 2 for $n \geq 3$ [4, p.104]. Applying lemma 1 we have

<u>LEMMA 2.</u> $1 + p^k$ (p a prime)is of period p^{n-k} in $M(p^n)$ and 2^k-1 is of period 2^{n-k} in $M(2^n)$ where $k \geq 1$ for $p \neq 2$

and $k \geq 2$ for $p = 2$.

Using lemma 2 we prove.

THEOREM 6: The groups $S(p^n, p^m, 1+p^h)$ where $h = Max(1,n-m),\ldots,n$ for $p \neq 2$ and the groups $S(2^n, 2^m, 2^h \pm 1)$ where $h = Max(2,n-m)\ldots,n$ are the only non-isomerphic groups $S(p^n, p^m, r)$ for any p(a prime), n and m.

PROOF: For $p \neq 2$ the group R is a cyclic subgroup of $M(p^n)$. R is generated by $1+p^k$ where $k = Max(1,n-m)$. Its cyclic subgroups are generated by $1+p^h$ where $h = k, \ldots, n$. The periods of any two of these generators are not equal. Hence the result follows for $p \neq 2$ by applying theorems 3 and 4.

For $p = 2$ the cyclic subgroups of $M(2^n)$ are generated by

$$5^{2^k} , - 5^{2^k} \quad \text{where} \quad k = 0,1,\ldots,n-2.$$

and $\pm 5^{2^k}$ are of period 2^{n-k-2} except $-5^{2^{n-2}} = -1$ which is of period 2. But $2^{k+1} \pm 1$ are of period

$$2^{n-k-2} \quad \text{and} \quad \left\{ 2^{k+2}-1 \right\} \neq \left\{ 2^{k+2}+1 \right\} .$$

Therefore the cyclic subgroups can also be generated by

$$2^h \pm 1 \quad \text{where} \quad h = 2,3,\ldots,n.$$

The generators r and r' of any two distinct cyclic subgroups $\{ r \}$, $\{ r' \}$ mentioned above have either unequal periods or $(r-1,2^n) \neq (r'-1,2^n)$ except $2^{n-1}-1$ and -1. $2^{n-1}-1$ is not

in the generators of the cyclic subgroups when $n < 3$ and its period is 2 as of -1 and $(2^{n-1} - 1 - 1, 2^n) = (-1-1, 2^n) = 2$ when $n \geq 3$. Hence theorem 4 cannot be applied here. However, we can prove that $S(2^n, 2^m, 2^{n-1}-1)$ and $S(2^n, 2^m, -1)$ are non-isomorphic for $n \geq 3$.

Suppose

$$S(2^n, 2^m, 2^{n-1}-1) = \{c, d\}$$

and

$$S(2^n, 2^m, -1) = \{a, b\}$$

are isomorphic. This will be given by

$$(c,d) \rightarrow (a^x b^y,\ a^z b^w)$$

$$dc \rightarrow a^{z+x(-1)^w}\ b^{w+y}$$

$$c^{2^{n-1}-1}\ d \rightarrow a^{x'}\ b^{w+y(2^n-1)}$$

where

$$x' = x[1+(-1)^y + \ldots + (-1)^{y(2^{n-1}-2)}] + z(-1)^{y(2^{n-1}-1)}.$$

From these we have

$$y(2^{n-1}-1) \equiv y \bmod 2^m \quad \text{or} \quad y \equiv 0 \bmod 2^{m-1}.$$

When $m > 1$ then y is even and therefore w is odd hence

$$z - x \equiv x' \bmod 2^m \quad \text{or} \quad -x \equiv (2^{n-1}-1)\, x \bmod 2^n$$

which implies $x \equiv \bmod 2$.

Therefore $y = f2^{n-1}$ and $x = 2 \cdot g$ where f and g are any two integers. But in this case $a^x b^y$ is of order at most 2^{n-1} since

$$(a^{2g}\ b^{f2^{n-1}})^{2^{n-1}} = a^{g2^n} = e.$$

Also when m = 1 then y = 0 or 1. If y = 0 then x should be even and a^x is of order 2^{n-1} at most. If y = 1 then

$$(a^x b)^2 = e.$$

Therefore for all cases, $a^x b^y$ is of order 2^{n-1} at most and

$$c \to a^x b^y$$

is not one to one since c is of order 2^n, $n \geq 3$, and therefore $S(2^n,2^m,2^{n-1}-1)$ is not isomorphic to $S(2^n,2^m,-1)$.

Now the group R is a subgroup of $M(2^n)$. Its cyclic subgroups are generated by

$$2^h \pm 1 \quad \text{where} \quad h = Max(2,n-m),\ldots,n.$$

Hence by applying the above result together with theorems 3 and 4 we arrive at the required result. This completes the proof of the theorem.

If M = Max(1,n-m) and M' = Max(2,n-m) then the number of distinct non-isomorphic groups of the form $S(p^n,p^m,r)$, p a prime, will be exactly equal to n - M + 1 when $p \neq 2$ and 2(n-M'+1) when p = 2.

p-groups are nilpotent and since $S(p^n,p^m,r)$ is a p-group of order p^{n+m} it should be nilpotent. From theorem 6 we see that $r \equiv 1 \bmod p$ and using theorem 2 we find that $S(p^n,p^m,r)$ is nilpotent. This gives another prrof. The proof that every p-group is nilpotent is found in most textbooks on group theory [2, p.155]. Its class can also

be found. Using sections 2 and 4 of chapter I we have $S(p^n,p^m,1+p^h)$ has the center $Z = \{a^{p^{n-h}}, b^{p^{n-h}}\}$ and the commutator subgroup $C = \{a^{p^h}\}$. It is nilpotent of class $\frac{n}{h}$ when $h|n$ and $[\frac{n}{h}] + 1$ when $h \nmid n$. However, $S(2^n,2^m,2^h-1)$ has the center $Z = \{a^{2^{n-1}}, b^{2^{n-h}}\}$ and the commutator subgroup $C = \{a^2\}$. It is nilpotent of class n.

Using theorem 6 we can study the group $A(p^n,p^m,r)$. Here r should satisfy the congruence,

$$r^{p^m-1} + r^{p^m-2} + \ldots + r + 1 \equiv 0 \bmod p^n.$$

Taking each r of theorem 6 and testing whether it satisfies the congruence is tedious. However, we can use lemma 1 and prove.

THEOREM 7: When $n \leq m$ then every group $S(p^n,p^m,r)$ satisfies the defining relations of $A(p^n,p^m,r)$. When $n > m$ then no groups $A(p^n,p^m,r)$ exists for $p \neq 2$ and for $p = 2$ only $A(2^n,2^m,2^h-1)$ where $h = n-m+1,\ldots,m$ exist.

PROOF: From lemma 1 we see that $p^{m+h} | (1+p^h)^{p^m}-1$. Fracterizing $(1+p^h)^{p^m}-1$ we get

$$p^h[(1+p^h)^{p^m-1} + \ldots + (1+p^h)+1].$$

Hence using the lemma one finds that the highest power of p(a prime) dividing $(1+p^h)^{p^m-1} + \ldots + (1+p^h)+1$ is p^m. Hence if $n \leq m$ and if $r = 1 + p^h$ then

$$r^{p^m-1} + r^{p^m-2} + \ldots + r + 1 \equiv (1+p^h)^{p^m-1} + \ldots + (1+p^h)+1 \equiv 0 \bmod p^n.$$

for $h = 1, \ldots, n$. However, if $n > m$ then there exists no $r = 1 + p^h$ such that the congruence above is satisfied.

$(2^h-1)^{2^m}-1$ satisfies lemma 1 too. i.e. the highest power of 2 that divides it is 2^{m+h} where $h \geq 2$.

Fractorizing $(2^h-1)^{2^m}-1$ we get

$$(2^h-2)[(2^h-1)^{2^m-1} + \ldots + (2^h-1)+1]$$

$$= 2(2^{h-1}-1)[(2^h-1)^{2^m-1} + \ldots + (2^h-1)+1].$$

Hence the highest power of 2 dividing

$$(2^h-1)^{2^m-1} + (2^h-1)^{2^m-2} + \ldots + (2^h-1)+1 \text{ is } 2^{m+h-1}$$

Therefore if $r = 2^h-1$ then

$$r^{2^m-1} + r^{2^m-2} + \ldots + r + 1 \equiv (2^h-1)^{2^m-1}+(2^h-1)^{2^m-2} + \ldots+(2^h-1)+1 \equiv 0 \bmod 2^n,$$

when $n \leq m$ the above congruence is true for every $h \geq 2$ and when $n > m$ then the above congruence is true only for $h = n - m + 1, \ldots, n$. Hence the result follows by applying theorem 6.

3. <u>The Group $A(q^n,p^m,r)$.</u>

In this section the case in which q and p are distinct primes will be studied. We first begin studying the group $S(q^n,p^m,r)$ which has the defining relations,

$$a^{q^n} = b^{p^m} = e, \quad ba = a^r b, \; r^{p^m} \equiv 1 \bmod q^n.$$

Suppose $(p,q-1) = 1$ then the only solution of

$$r^{p^m} \equiv 1 \bmod q^n$$

is $r = 1$ since the group $M(q^n)$ does not have an element of order p. Hence only $S(q^n,p^m,1)$ exists in this case.

On the other hand suppose $(p^m,q-1) = p^s$ where $s \leq m$ then the group R is a subgroup of $M(q^n)$, it is cyclic of order p^s. Hence R has a generator, say g. Using theorems 3 and 4 we conclude that the only non-isomorphic distinct groups of the form $S(q^n,p^m,r)$ are for $r = g^{p^h}$, $h = 0, 1, \ldots, s$.

Now we use only these values of r and see which of them satisfy the relation

$$1 + r + r^2 + \ldots + r^{p^m-1} \equiv 0 \bmod q^n.$$

Since p and q are distinct primes $r = 1$ does not satisfy the above congruence. Hence there exist no groups $A(q^n,p^m,r)$ if $(p,q-1) = 1$. However, if $(p^m,q-1) = p^s \neq 1$ then g, as defined above, is not equal to 1, and only $g^{p^s} \equiv 1 \bmod q^n$. Hence $(g^{p^h}-1,q) = 1$ for $h < s$. Therefore if $r = g \neq 1$ satisfies $r^{p^m} \equiv 1 \bmod q^n$ then it also satisfies $1 + r + r^2 + \ldots + r^{p^m-1} \equiv 0 \bmod q^n$ and we conclude that the only non-isomorphic distinct groups of the form $A(q^n,p^m,r)$ are for values of $r = g^{p^h}$, $h = 0, 1, \ldots, s - 1$.

Note here that the number of the above groups depends on $(p^m,q-1)=p^s$ and is independent of n. If $m > s$

then r and the number of groups are independent of m and depend on s.

The above results will be illustrated by the following example. Consider the group $S(19^n,3^m,r)$ with the defining relations

$$a^{19^n} = b^{3^m} = e,\ ba = a^r b.$$

Since

$$(3,19-1) = 3 \text{ and } (3^m,19-1) = 3^2 \text{ for } m > 1$$

then there exist two such groups when $m = 1$ and three when $m > 1$. To find all these groups note that $M(19) = \{2\}$. Also since $2^{18} \not\equiv 1 \bmod (19)^2$ then $M(19^n) = \{2\}$ for any n [4, p.107]. The group R is generated by $2^{2\cdot 19^{n-1}}$ when $m \geq 2$ and by $2^{6\cdot 19^{n-1}}$ when $m = 1$. Hence we have

$$S(19^n,3^m,1),\ S(19^n,3^m,2^{2\cdot 19^{n-1}}),\ \text{and}\ S(19^n,3^m,2^{6\cdot 19^{n-1}})$$

where the middle group does not exist for $m = 1$, as all the non-isomorphic groups of the form $S(19^n,3^m,r)$ possible. Every non-Abelian group mentioned above satisfies the relations of $A(19^n,3^m,r)$,

i.e.

$$a^{19^n} = b^{3^m} = (ab)^{3^m} = e,\ ba = a^r b.$$

4. Generalizations.

For a given pair of integers n and m we can find the corresponding group R and by applying theorems 3 and 4 the groups S(n,m,r) can be found. Also if we apply the first section of this chapter we will be able to find the

groups A(n,m,r). However, it will not be easy to formulate a rule that will discover all the groups S(n,m,r) or A(n,m,r) for any n and m since R in this case might be an Abelian group which is not cyclic. In fact R might be a very complicated Abelian group. In section one we found that A(n,m,r) always exists when m is even but not necessarily when m is odd. Using the preceding sections we will find the necessary and sufficient conditions for the existence of A(n,m,r).

Let us first mention a theorem in number theory that will be helpful. If $n = p_o^{e_o} p_1^{e_1} \dots p_s^{e_s}$ and N(m) is the number of solutions of $f(r) \equiv 0 \bmod m$ then

$$N(n) = N(p_o^{e_o})N(p_1^{e_1}) \dots N(p_s^{e_s}). \quad [3, p.39].$$

In the group A(n,m,r), which has the defining relations,

$$a^n = b^m = (ab)^m = e \quad ba = a^r b.$$

r should satisfy the congruence

$$1 + r + \dots + r^{m-1} \equiv 0 \bmod n . \dots\dots\dots (1)$$

If p^h is the highest power of a prime p dividing n, then by applying the above theorem (1) will have solutions if and only if

$$1 + r + \dots + r^{m-1} \equiv 0 \bmod p^h \dots\dots\dots (2),$$

has a solution for every prime power factor of n [3, p.38].

r should also satisfy the congruence,

$$r^m \equiv 1 \bmod p^h . \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Suppose $(m,p^h) = p^h$ then $m = kp^h$ and all the solutions of $r^{p^h} \equiv 1 \bmod p^h$ satisfy (3) and

$$1 + r + \ldots + r^{p^h-1} \equiv 0 \bmod p^h$$

and

$$1 + r + \ldots + r^{m-1} \equiv r + \ldots + r^m$$

$$\equiv r + \ldots + r^{p^h} + \ldots + r^{kp^h}$$

$$\equiv k(1+r+\ldots+r^{p^h-1}) \equiv 0 \bmod p^h .$$

Hence these solutions satisfy (2).

Now suppose $(m,p-1) \neq 1$, then there exists a prime $q|m$ and $q|p-1$. Hence by section 3 an integer $g > 1$ exists such that $g^q \equiv g^m \equiv 1 \bmod p^h$ and $(g-1,p) = 1$ since g does not generate a group of order a power of p. Hence g will satisfy (2).

On the other hand suppose $(m,p^h) = p^s$, $s < h$, and $(m,p-1) = 1$, then $r^{p^s} \equiv 1 \bmod p^h$ will have the same solutions as (3) since $(\frac{m}{p^s}, p) = 1$. In fact $(\frac{m}{p^s}, \phi(p^h)) = 1$. By section 2, none of these solutions satisfies

$$1 + r^2 + \ldots + r^{p^s-1} \equiv 0 \bmod p^h \quad h > s.$$

Now (2) can be written as

$$\frac{m}{p^s} (1 + r + r^2 + \ldots + r^{p^s-1}) \equiv 0 \bmod p^h .$$

Therefore (2) has no solutions.

The above discussion can be sumarized as,

THEOREM 8: For $A(n,m,r)$ to exist it is necessary and sufficient that at least one of the followings is satisfied,

1. m is even.
2. For every prime p such that $p^h | n$ and $p^{h+1} \nmid n$, $h > 0$, if $(p^h, m) = p^s$ and $(m, p-1) = g$ then $s = h$ or $g > 1$.

If we apply this theorem to $A(n,p^m,r)$ (p odd) it becomes the following statement,

For $A(n,p^m,r)$, p an odd prime, to exist it is necessary and sufficient that $p^{m+1} \nmid n$ and if q is any prime such that $q|n$ and $q \neq p$ then $q \equiv 1 \bmod p$.

In this case we see that p is the smallest prime factor of n, in fact all the other prime factors of n distinct from p are in the set $\{2kp + 1 \; ; \; k = 1, 2, 3, \ldots\}$. Since $(2p,1) = 1$ then by applying Dirichlet's theorem we find that this set has infinitely many primes. Hence there exist infinitely many integers n for which $A(n,m,r)$ exists, for any given m.

5. The Group $A(n,p^m,r)$.

The theorems proved so far can be used to get interesting results. For instance all the groups $S(n,p^m,r)$ can be found for any prime p such that $(n,p) = 1$. Suppose

$$n = kp_1^{n_1} \ldots p_s^{n_s} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

where $(n,p) = (k,p_i) = 1$, $p_i \equiv 1 \bmod p$ for $i = 1, \ldots, s$; and if q is a prime dividing k then $q \not\equiv 1 \bmod p$. To find the groups $S(n,p^m,r)$ we should solve the congruence,

$$r^{p^m} \equiv 1 \bmod n ,$$

which holds if and only if the congruences

$$r^{p^m} \equiv 1 \bmod k, \text{ and } r^{p^m} \equiv 1 \bmod p_i^{n_i} \text{ for } i = 1, \ldots, s$$

hold [3, p.38].

The number of solutions of the first congruence is equal to the product of the numbers of solutions of the congruences given above. If we suppose that

$$m = 1 \text{ or } (p_i - 1, p^m) = p \text{ for } m > 1 \text{ and } i = 1, \ldots, s \quad \ldots(2)$$

then the group R will be an elementary Abelian group of order p^s since $r^{p^m} \equiv 1 \bmod k$ has only one solution. R contains $p^{s-1} + p^{s-2} + \ldots + p + 1$ distinct cyclic subgroups of order p and the cyclic subgroup $\{1\}$. Theorems 3 and 4 can be applied. Here there exist exactly $p^{s-1} + p^{s-2} + \ldots + p + 2$ non-isomorphic groups of the form $S(n,p^m,r)$. To find all these groups we define k_i and h_i as follows,

$$\frac{n}{k} k_o \equiv 1 \bmod k , \quad \frac{n\,k_i}{p_i^{n_i}} \equiv 1 \bmod p_i^{n_i} \text{ for } i > 0 \qquad \ldots\ldots\ldots(3)$$

$$h_o = \frac{n}{k} k_o \text{ and } h_i = \frac{n}{p_i^{n_i}} k_i \text{ for } i > 0$$

By section 3, g_i for $i = 0, 1, \ldots, s$ can be found such that

$$g_o = 1, \quad g_i^p \equiv 1 \bmod p_i^{n_i}$$

and

$$g_i \not\equiv 1 \bmod p_i^{n_i} \quad \text{for } i > 0 \qquad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

By the Chinese remainder theorem the solutions of

$$r^{p^m} \equiv 1 \bmod n$$

will be $r = \sum_{i=0}^{s} g_i^{e_i} h_i$ where $e_o = 0$ and $e_i = 1, \ldots, p$. $i > 0$.

To find the cyclic subgroups of R, first note that

$$\left[\sum_{i=0}^{s} g_i^{e_i} h_i\right]^f \equiv \sum_{i=0}^{s} g_i^{e_i} h_i^f \bmod n$$

since

$$h_i h_j \equiv 0 \bmod n \quad \text{for } i \neq j.$$

Also

$$h_i \equiv 1 \bmod p_i^{n_i}, \text{ i.e. } p_i^{n_i} | h_i - 1.$$

Multiplying both sides by h_i we get

$$h_i p_i^{n_i} = k_i n | h_i(h_i - 1) = h_i^2 - h_i$$

or

$$h_i^2 \equiv h_i \bmod n.$$

Hence

$$h_i^f \equiv h_i^{f-1} \equiv \ldots \equiv h_i \bmod n$$

and we have

$$r^f = \sum_{i=0}^{s} g_i^{fe_i} h_i.$$

Note that if $e_j = p$ for some j then we can replace $g_i^{fe_i}$

by 1, i.e. fe_i by p. Also if

$$r' = \sum_{i=0}^{s} g_i^{f_i} h_i$$

then r' is a power of r if and only if there exists an integer f such that

$$fe_i \equiv f_i \bmod p \quad \text{for } i > 0.$$

Suppose t of the integers $e_i (i > 0)$ are equal to p, t can take the values 0, 1, ..., s. For each t we have $\binom{s}{t}$ different ways of choosing the t integers e_i equal to p. For any r and r' having these different ways of choosing p the congruence above is not satisfied for at least one pair of integers e_i and f_i. Now taking one of the choices, that is, fixing t and the integers which are equal to p, and setting $e_j = 1$ where $e_j \neq p$ then we will have $(p-1)^{s-t-1}$ r's in which no r is a power of any other. Hence for a fixed t we have

$$\binom{s}{t}(p-1)^{s-t-1}, \quad (t \leq s-1)$$

r's in which no r is a power of any other. All together there are

$$1 + \sum_{t=0}^{s-1} \binom{s}{t} (p-1)^{s-t-1}$$

such r's. This can be shown to be equal to

$$p^{s-1} + p^{s-2} + \ldots + p + 2.$$

Hence we have proved

THEOREM 9: If n,m,h_i, and g_i are as given in relations (1), (2), (3), and (4) then there exist exactly $p^{s-1} + p^{s-2} + \ldots + p + 2$ non-isomorphic groups $S(n,p^m,r)$. Here $r = \sum_{i=0}^{s} g_i^{e_i} h_i$ where $e_o = 0$, any $t(= 0, 1, \ldots, s)$ of the integers e_i equal to p, an integer $e_j = 1$, and the rest have values $1, 2, \ldots, p - 1$.

This theorem can be applied to find all groups of the form $A(n,p^m,r)$. Using theorem 8 n, h_i, g_i should now be given by the relations

$$n = p_o^{n_o} p_1^{n_1} \ldots p_s^{n_s}, \quad p_o = p \qquad \ldots\ldots\ldots\ldots(1')$$

$$p_i \equiv 1 \bmod p \quad \text{for } i > 0.$$

$$\frac{n}{p_i^{n_i}} k_i \equiv 1 \bmod p_i^{n_i} \quad \text{and} \quad h_i = \frac{n}{p_i^{n_i}} k_i \qquad \ldots\ldots\ldots(3')$$

$$g_o = 1 + p, \quad g_i^p \equiv 1 \bmod p_i^{n_i}, \qquad \ldots\ldots\ldots(4')$$

and

$$g_i \not\equiv 1 \bmod p_i^{n_i} \quad \text{for} \quad i = 1, \ldots, s$$

THEOREM 10: If n,m,h_i and g_i are given as in relations (1'), (2), (3') and (4') then there exist exactly $(p-1)^{s-1}$, $[p(p-1)^{s-1}]$, non-isomorphic groups $A(n,p^m,r)$ when $n_o = 0$ or 1, $[n_o = 2]$. Here $r = \sum_{i=0}^{s} g_i^{e_i} h_i$ where $e_o = 0, [e_o = 1, \ldots, p]$, $e_1 = 1$, and $e_i = 1, \ldots, p - 1$ for $i > 1$.

PROOF: The congruences that should be solved now are

$$r^{p^m-1} + r^{p^m-2} + \ldots + r + 1 \equiv 0 \bmod p_i^{n_i}, \quad i = 0, 1, \ldots, s.$$

If $p_i \nmid p$ then by section 3 the above congruence has the solutions $g_i, g_i^2, \ldots, g_i^{p-1}$; i.e., g_i^p is not a solution. Hence if $n_o = 0$ then the result follows at once from the previous theorem. However, if $n_o > 0$ then theorem 4 can no more be applied and we should prove that if $A(n,p^m,r_1) \cong A(n,p^m,r_2)$ then $\{r_1\} = \{r_2\}$.

Since the case where n is a power of p was studied in section 2 we suppose that n has at least one prime factor $p_i \nmid p$. Suppose $A(n,p^m,r_1) = \{a,b\}$ and $A(n,p^m,r_2) = \{c,d\}$ and the isomorphism given by

$$(a,b) \to (c^x d^y,\ c^z d^w).$$

If $(y,p) = 1$ then

$$(c^x d^y)^{p^m} = c^{x(1+r_2^y+\ldots+r_2^{y(p^m-1)})}\ b^{yp^m} = e.$$

But a is of order n and this is not possible. Therefore $y \equiv 0 \bmod p$, also $(w,p) = 1$ for otherwise $\{c^x d^y,\ c^z d^w\}$ would be an Abelian group. Also

$$ba = a^{r_1} b \to c^z d^w\ c^x d^y = a^{z+xr_2^w}\ d^{w+y}$$

$$a^{r_1} b \to c^{xr_1 + z}\ d^{r_1 y + w}$$

Hence

$$xr_1 \equiv xr_2^w \bmod n .$$

$(x,n) = 1$ for otherwise $\{c\}$ would not be contained in $\{c^x d^y,\ c^z d^w\}$. Therefore the above congruence becomes

$$r_1 \equiv r_2^w \bmod n .$$

By theorem 4 the periods of r_1 and r_2 are equal, hence $\{r_1\} = \{r_2\}$. The results for $n_o = 1$, and 2 now can be proved using a similar method as in theorem 9.

Theorems 9 and 10 formulate rules to find all the groups $S(n,p^m,r)$ and $A(n,p^m,r)$ without solving any congruences.

For instance to find all the non-isomorphic groups $S(91,3^m,r)$ we first find g_i, h_i, k_i for $i = 1$, and 2 since $91 = 7 \times 13$. These are given by

$g_1 = 2$, $g_2 = 3$, $k_1 = -1$, $k_2 = 2$, $h_1 = -13$, and $h_2 = 14$.

If

$$r_{ij} = -13.2^i + 14.3^j$$

then applying theorem 9 we see that there exist 5 non-isomorphic groups $S(91,3^m,r)$ for the following values of r

$$r_{11} = 16,\ r_{12} = 9,\ r_{13} = -12,\ r_{31} = 29,\ r_{33} = 1.$$

To find all the groups $A(91,3^m,r)$ note that i and j should be different from three in r_{ij}. By theorem 10 there are two group $A(91,3^m,r)$ for $r_{11} = 16$ and $r_{12} = 9$.

Theorem 10 formulates a method by which groups $A(n,p^m,r)$ can be found without even finding $S(n,p^m,r)$. To illustrate this we find all the groups $A(819,3^m,r)$ where $m \geq 2$ and $819 = 3^2.7.13$. Here g_i, h_i for $i = 0$, 1, and 2 are given by

$g_o = 4$, $g_1 = 2$, $g_2 = 3$, $h_o = 91$, $h_1 = 351$ and $h_2 = 378$.

If

$$r_{ij} = 91.4^i + 351.2^j + 378.3$$

then by theorem 10 there are 6 non-isomorphic groups $A(819, 3^m, r)$ for $r = r_{ij}$, $i = 1, 2, 3$, and $j = 1, 2$. These are for the values of r given below

$$r_{11} = -257,\ r_{21} = 16,\ r_{31} = 289$$

$$r_{12} = 445,\ \ r_{22} = -101, r_{32} = 172.$$

Note that the smallest value of n such that there exist two distinct groups $A(n,3^m,r)$, different from p-groups, is 91, that for three groups is 63 (here the values of r are given by -5, 4, 9) and that for six groups is 819. In fact this can be generalized. By Dirichlet's theorem there exist infinitely many primes in the set

$$\{ 1 + p,\ 1 + 2p + \ldots + 1 + sp + \ldots \}.$$

Choose the first $s + 1$ primes of this set, say $p_1, p_2, \ldots, p_{s+1}$ then the smallest value of n such that there exist $(p-1)^s$ distinct groups $A(n,p,r)$ is $n = p_1 p_2 \cdots p_{s+1}$. And if these primes can be chosen such that $(p_i - 1, p^m) = p$ for $m \geq 2$ then the smallest n such that there exist $p(p-1)^s$ distinct group $A(n,p^m,r)$, not p-groups, is $p^2 p_1 p_2 \cdots p_{s+1}$ where $m \geq 2$.

CHAPTER III

INFINITE GROUPS

1. Introduction.

This paper will remain incomplete if a short chapter is not devoted to some remarks on infinite groups of two generators, of which at least one is of infinite order. Some of the properties of the finite groups found in the previous chapters can be extended to the infinite groups with no changes, others need slight modifications. To get interesting groups we need to change some of the relations between the generators.

Suppose the infinite cyclic groups $\{a\}$ and $\{b\}$ have the relations

$$a^n = b^m, \quad ba = a^r b,$$

where n and m are any non-zero integers.

Since

$$bb^m = ba^n = a^{nr} b = a^n b$$

then

$$nr = n \quad \text{or} \quad r = 1.$$

Therefore the set

$$G(\infty,\infty,1) = \left\{ a^i b^j : i = 0, \pm 1, \pm 2, \ldots, j = 0, 1, \ldots, m-1 \right\}$$

is an Abelian group since it satisfies the axioms of a group and its two generators commute.

However, suppose the relations are

$$ba^n = a^n b,\ ba = a^r b.$$

Then $r = 1$ and the set

$$S(\infty,\infty,1) = \left\{ a^i b^j : i,j = 0, \pm 1, \pm 2, \ldots \right\}$$

forms an Abelian group which is the direct product of two infinite cyclic groups. Note that

$$G(\infty,\infty,1) \cong S(\infty,\infty,1)/K$$

where

$$K = \left\{ a^n\ b^{-m} \right\}.$$

If we let a commute with a power of b,i.e.,

$$b^m a = ab^m,\ ba = a^r\ b$$

then

$$b^m a = a^{r^m}\ b^m = ab^m$$

which implies

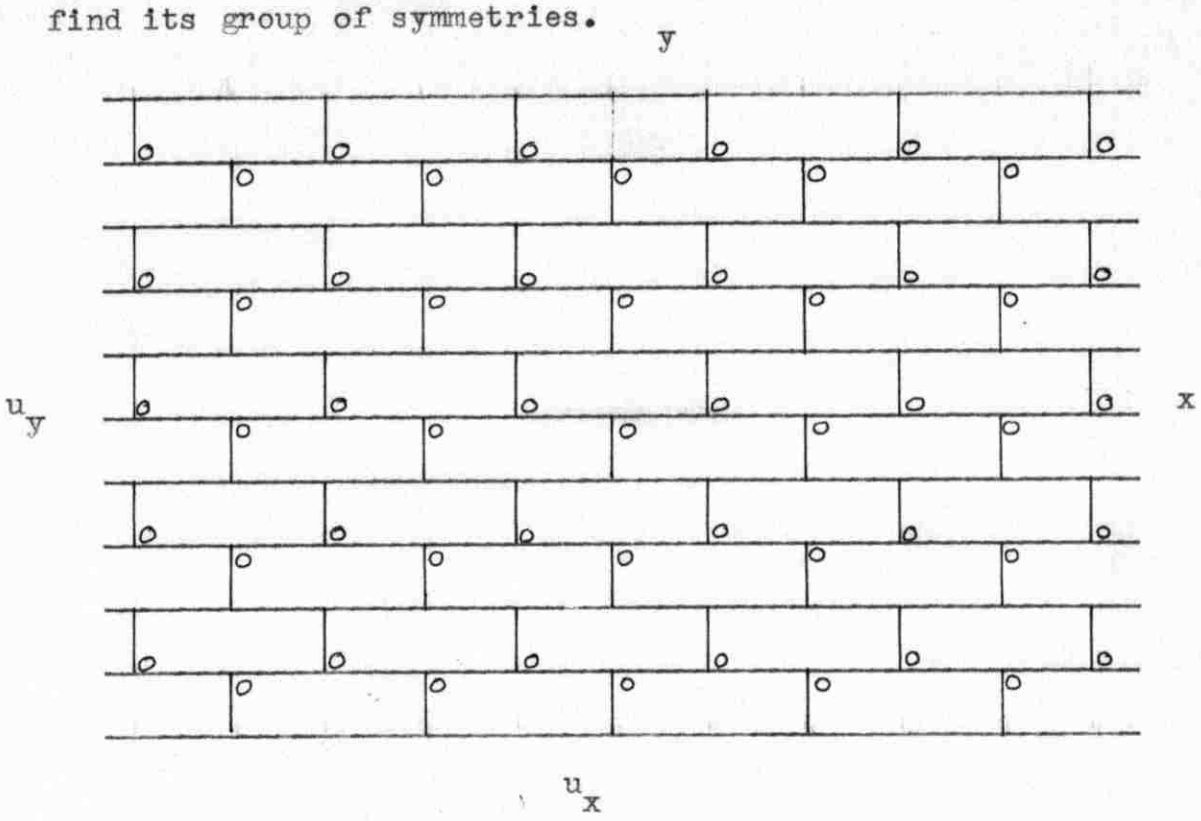
$$r^m = 1.$$

If m is odd then $r = 1$ is the only solution and $S(\infty,\infty,1)$ will be the only group possible. If m is even the $r = -1$ is another solution and we will have $S(\infty,\infty,-1)$ as another group. Hence $S(\infty,\infty,-1)$ is a non-Abelian group of two generators of infinite order having the relation $ba = a^{-1}b$. Here a generates a normal subgroup. Further properties of $S(\infty,\infty,-1)$ will be studied in the next section.

2. Properties of $S(\infty,\infty,-1)$.

Let us study the infinite pattern given below and

find its group of symmetries.



Let g be a glide reflection formed by a translation of one unit, u_x, along the x-axis and then a reflection in the line y = 0, and t a translation of two units, $2u_y$, along the y-axis. A glide reflection in the line y = n, where n is any integer, is given by

$$gt^n = t^{-n} g.$$

Hence the group of symmetries of the above figure is $\{g,t\}$ with $gt = t^{-1} g$. This is isomorphic to $S(\infty,\infty,-1)$.

The center Z can be found by considering all the elements of $S(\infty,\infty,-1)$ which commute with every other element, i.e., if $a^x b^y$ is in Z then

$$a^z b^w a^x b^y b^{-w} a^{-z} = a^x b^y \text{ for any } z \text{ and } w$$

which implies

$$z + x(-1)^w - z(-1)^y = x.$$

Since z and w are independent variables, the above equations gives $x = 0$ and $y = 0, 2, 4, \ldots$. Hence

$$Z = \{ b^2 \}.$$

$S(\infty,\infty,-1)/_Z$ consists of the cosets

$$\ldots \quad Za^{-2}, \; Za^{-1}, \; Z, \; Za, \; Za^2, \; \ldots$$

$$\ldots \quad Za^{-2}b, Za^{-1}b, Zb, Zab, Za^2b, \ldots$$

with Za of infinite order, $(Zb)^2 = Z$ and

$$(Zb)(Za) = Zba = Za^{-1}b = (Za)^{-1}(Zb).$$

Therefore $S(\infty,\infty,-1)/Z$ is isomorphic to $S(\infty,2,-1)$ which is known as the infinite dihedral group, usually denoted by D_∞.

$K = \{ b^{2m} \}$ is a subgroup of the center Z, for any m. Hence K is normal in $S(\infty,\infty,-1)$ and $S(\infty,\infty,-1)/K$ is isomorphic to $S(\infty,2m,-1)$. This has the defining relations

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

In fact when m is odd there exists only the Abelian group of the form $S(\infty,m,1)$ and when m is even there exist an

Abelian group of the form $S(\infty,m,1)$ and a non-Abelian one $S(\infty,m,-1)$.

To find the commutator subgroup C of $S(\infty,\infty,-1)$ consider a general commutator

$$a^{x}b^{y}a^{z}b^{w}b^{-y}a^{-x}b^{-w}a^{-z}$$

$$= a^{x+z(-1)^{y}-x(-1)^{w}-z}$$

$$= a^{2s} \quad , \text{ s an integer.}$$

But $aba^{-1}b^{-1} = a^2$ is in C. Hence C is cyclic and

$$C = \{a^2\}.$$

$S(\infty,\infty,-1)/C$ consists of

$$\ldots \quad Cb^{-2}, Cb^{-1}, C, Cb, Cb^2, \ldots$$

$$\ldots \quad Cab^{-2}, Cab^{-1}, Ca, Cab, Cab^2, \ldots$$

which is the direct product of two cyclic groups, one of infinite order the other of order 2.

Let $H = \{a^n, b^{2m}\}$ then H is normal in $S(\infty,\infty,-1)$ for any n and m. Let n and m be different from zero then $S(\infty,\infty,-1)/H$ consists of

$$\begin{array}{cccc} H, & Ha, & Ha^2, \ldots, & Ha^{n-1} \\ Hb, & Hab, & Ha^2b, \ldots, & Ha^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ Hb^{2m-1}, & Hab^{2m-1}, & Ha^2b^{2m-1}, \ldots, & Ha^{n-1}b^{2m-1} \end{array}$$

where $(Ha)^n = (Hb)^{2m} = H$, $(Hb)(Ha) = (Ha)^{-1}(Hb)$.

Therefore $S(\infty,\infty,-1)/H$ is isomorphic to $S(n,2m,-1)$. When $m = 1$ $S(n,2,-1)$ is known as the Dihederal group usually denoted by D_n.

Also if we let $L = \{ a^k b^{2h}, a^k b^{-2h} \}$ then L is normal in $S(\infty,\infty,-1)$ for any k and h. If k and h are not equal to zero then the factor group $S(\infty,\infty,-1)/L$ consists of

$$\begin{array}{cccc} L, & La, & La^2, \ldots, & La^{2k-1} \\ Lb, & Lab, & La^2b, \ldots, & La^{2k-1}b \\ \vdots & \vdots & \vdots & \vdots \\ Lb^{2h-1}, & Lab^{2h-1}, & La^2b^{2h-1}, \ldots, & La^{2k-1}b^{2h-1} \end{array}$$

where $(La)^{2k} = (Lb)^{4h} = L$, $(La)^k = (Lb)^{2h}$,

$$(Lb)(La) = (La)^{-1}(Lb).$$

Hence $S(\infty,\infty,-1)/L$ is isomorphic to $G(2k,4h,-1)$. Note that $G(2.2^n,2^2,-1)$ is known as the generalized quaternion group.

3. <u>The Group $S(n,\infty,r)$.</u>

Groups in which the generator b is of finite order has been considered in section 2 as a factor group of $S(\infty,\infty,-1)$. Some interesting results can be found when we let a, of finite order, commute with a power of b, of infinite order,

i.e.

$$a^n = e,\ b^m a = ab^m,\ ba = a^r b$$

This will give

$$r^m \equiv 1 \bmod n .$$

The set

$$S(n,\infty,r) = \{ a^i b^j : i=0,1,\ldots,n-1,\ j=0,\pm1,\pm2,\ldots \}$$

satisfies the axioms of a group. The set of all r's satisfying the above congruence forms the Abelian group R. Using similar method to these in section 2 chapter 1 we get

$$Z = \left\{ \frac{n}{a^{(r-1,n)}} , {}_b t \right\} \text{ and } C = \{ a^{r-1} \} .$$

Conditions for $S(n,\infty,r)$ to be nilpotent and its class are exactly the same as those of $G(n,m,r)$ found in section 4 of chapter 1. However, the isomorphism theorems proved previously will not apply for $S(n,\infty,r)$. In fact we have

THEOREM 11: For distinct r and r' $S(n,\infty,r) \cong S(n,\infty,r')$ if and only if $rr' \equiv 1 \bmod n$.

PROOF: Let $S(n,\infty,r) = \{ a,b \}$ and $S(n,\infty,r') = \{ c,d \}$.
The isomorphism $(a,b) \to (c,d^{-1})$
would hold if

$$ba \to d^{-1}c = c^{r'-1} d^{-1}$$

$$a^r b \to c^r d^{-1} .$$

i.e. if $r \equiv r'^{-1} \bmod n$ or $rr' \equiv 1 \bmod n$.

On the other hand suppose $S(n,\infty,r)$ and $S(n,\infty,r')$

are isomorphic and the isomorphism is given by

$$(a,b) \to (c^x d^y,\ c^z d^w).$$

If $y \neq 0$ then $c^x d^y$ is of infinite order, hence $y = 0$ and $(x,n) = 1$. Also if $w \neq \pm 1$ then $\{ d \}$ would not be contained in $\{ c^x,\ c^z d^w \}$. Therefore the isomorphism should be

$$(a,b) \to (c^x,\ c^z d^w) \qquad \text{where } w = \pm 1.$$

Now

$$ba \to c^z\ d^w\ c^x = c^{z+xr^{\pm w}}\ d^w$$

$$a^r b \to c^{xr+z}\ d^w.$$

Hence

$$r \equiv r'^{\pm 1} \bmod n .$$

Since $r \not\equiv r' \bmod n$ it follows that

$$rr' \equiv 1 \bmod n .$$

Using the above theorem we see that $S(n,\infty,r)$ and $S(n,\infty,r^f)$ are not isomorphic if $f \not\equiv \pm 1 \bmod t$ where t is the period of r. However, if $H = \{ a,b^f \}$ is a subgroup of $S(n,\infty,r)$ then H is isomorphic to $S(n,\infty,r^f) = \{ c,d \}$. In fact this is given by

$$(c,d) \to (a,b^f).$$

Also if $S(n,\infty,r') = \{ c,d \}$ is isomorphic to a subgroup of $S(n,\infty,r) = \{ a,b \}$ the r' should be a power of r for suppose

the isomorphism is given by

$$(c,d) \rightarrow (a^x,\ a^z b^y),\ (x,n) = 1$$

then

$$dc \rightarrow a^z\ b^y\ a^x = a^{z+xr^y}\ b^y$$

$$c^{r'}d \rightarrow a^{z+xr'}\ d^y$$

and

$$r' \equiv r^y \bmod n\ .$$

This result can be stated as

COROLLARY: $S(n,\infty,r')$ is isomorphic to a subgroup of $S(n,\infty,r)$ if and only if $\{r'\} \subseteq \{r\}$.

Note that if $\{r'\} = \{r\}$ then $S(n,\infty,r')$ is isomorphic to a subgroup of $S(n,\infty,r)$ and conversely, but they will not be isomorphic if the condition of theorem 11 is not satisfied. In particular every group $S(n,\infty,r)$ is isomorphic to its subgroup $\{a,b^h\}$ where $h \equiv 1 \bmod t$.

Theorem 11 can be applied to find all the non-isomorphic groups $S(n,\infty,r)$. If R is of odd order $2k+1$ then the identity 1 is the only element which is its own inverse, and the number of distinct groups $S(n,\infty,r)$ will be $k + 1$. If R is of even order $2k$, then by the theorem of Frobenius there are $2h$, $h \leq k$, elements of R that are their own inverses [2, p.137]. The number of non-isomorphic groups $S(n,\infty,r)$ will be $k + h$.

However, if we want to find the set of all groups $S(n,\infty,r)$ such that no group is isomorphic to a subgroup of

another, then we should find the generators of all the cyclic subgroups, $C_1, C_2, \ldots, C_s$, of R such that $C_i \cap C_j = N_{ij}$ where N_{ij} is a proper subgroup of C_i and C_j for $i \neq j$. Note that the Abelian group $S(n,\infty,1)$ will not be in this set if R has more than one element. In this case $S(n,\infty,1)$ is isomorphic to a subgroup of every other group. If R is a cyclic group, say $R = \{g\}$, then $S(n,\infty,g)$ is the only element of this set. In particular every group $S(p^n,\infty,r)$, where p is an odd prime, is isomorphic to a subgroup of $S(p^n,\infty,g)$ where $M(p^n) = \{g\}$.

Suppose there exists an integer k dividing n such that $kr \equiv k \bmod n$. Since $(r,n) = 1$ there exists another integer h such that $r^h \equiv 1 \bmod n$. In what follows h is not assumed to be the smallest such integer. The subgroup $K = \{a^k b^h, a^k b^{-h}\}$ is normal in $S(n,\infty,r)$ and the factor group $S(n,\infty,r)/K$ consists of the cosets

$$K, \quad Ka, \quad Ka^2, \ldots, Ka^{n-1}$$

$$Kb, \quad Kab, \quad Ka^2b, \ldots, Ka^{n-1}b$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$Kb^{h-1}, Kab^{h-1}, Ka^2b^{h-1}, \ldots, Ka^{n-1}b^{h-1}$$

where

$$(Ka)^n = (Kb)^{hn/k} = K, \quad (Ka)^k = (Kb)^h,$$

and

$$(Kb)(Ka) = (Ka)^r(Kb).$$

Therefore $S(n,\infty,r)/K$ is isomorphic to $G(n,h\frac{n}{k},r)$.

Let the defining relations of $S(n,\infty,r)$ be

$$a^n = e \quad b^m a = ab^m \quad \text{where} \quad m = \phi(n).$$

Then for a fixed n and any other value of m, every group $S(n,\infty,r)$, is isomorphic to one of the groups having the above defining relations.

BIBLIOGRAPHY

Group Theory

1. Ledermann, W., Introduction to the Theory of Finite Groups. 3rd ed. Edinburgh, Oliver and Boyd, Ltd.,1957.

2. Hall, M. Jr., The Theory of Groups. 1st ed. New York, The Macmillan Company, 1959.

Number Theory

3. Niven and Zuckerman,An Introduction to the Theory of Numbers. 1st ed. New York, John Wiley and Sons, Inc., 1960.

4. Nagell, T., Introduction to Number Theory. 1st ed. New York, John Wiley and Sons, Inc., 1951.

5. Le Veque, W. J., Topics in Number Theory. v. 2, 1st ed. Reading, Mass., Addison-Wesley Publication Company, Inc., 1956.

INDEX OF SPECIAL SYMBOLS

Σ Summation sign, 33

$\#$ Congruent, 2

$\cong$ Isomorphic, 8

$\rightarrow$ One to one mapping, 16

$|$ divides, 1

$\cap$ Intersection, 5

$\supseteq$ Contains, 12

$\subseteq$ Is contained in, 60