SOME PROPERTIES OF DIHEDRAL AND ANALOGOUS GROUPS HAVING TWO GENERATORS

By

Ali Abdul-Latif

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

1961

TWO ANALOGOUS GROUPS

Ali Abdul-Latif

SOME PROPERTIES OF DIHEDRAL AND ANALOGOUS GROUPS HAVING TWO GENERATORS

By

Ali Abdul-Latif

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
1961

ACKNOWLEDGEMENTS

The writer wishes to express his deepest gratitude to Professor P. Yff, whose generous donation of time and supply of material during the summer of 1960 made possible beginning the study of the subject, and whose most valuable advice during the academic year of 1960-61 made this work possible.

He is also indebted to Mrs. K. Shomar, and would like to thank her for her patience and skill in typing the manuscript.

ABSTRACT

The dihedral group is a well known group which is mentioned in most books on finite groups.

The problems considered in this thesis deal with some of the properties of the dihedral group and an analogous group which has a generator of order 3 instead of one of order 2. The properties are investigated for both groups in an analogous manner.

These properties are: existence, the center, the factor group with respect to the center, the commutator subgroup, the factor group with respect to the commutator subgroups, Sylow subgroups, and the group of automorphisms. A special attempt was made to describe the group of automorphisms and some of its subgroups.

TABLE OF CONTENTS

page

CHAPTER I

INTRODUCTION

1. Remarks

A general knowledge of elementary finite group theory and elementary number theory is presupposed.

Chapter II of thesis is concerned with some of the properties of the dihedral group and in particular the group of automorphisms of the dihedral group.

Chapter III is concerned with properties of an analogue of the dihedral group in which there is a generator of order 3 instead of one of order 2. The properties of this group will be investigated in an analogous manner with those of the dihedral group.

2. Notations

The following notations have been used throughout the thesis:

D_n = Dihedral group of order 2n.

G_n = Analogue group of order 3n.

Z = The center of any group under discussion.

C = The commutator subgroup of any group under discussion.

$A(G)$ = The group of automorphisms of any group G.

$I(G)$ = The group of inner automorphisms of any group G.

$A \sim B$ = The groups A and B are isomorphic.

$\{b\}$ = The cyclic group generated by the element b.

$\{a,b\}$ = The group generated by the two elements a and b.

$\{A,B\}$ = The group generated by the two groups A and B.

$\{A,a\}$ = The group generated by the group A and the element a.

$[a_1,a_2,\ldots,a_n]$ = The group whose elements are $a_1,a_2,\ldots,$ and a_n.

$\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ = The permutation which takes a_i to b_i, here the permutation is an element of a permutation group.

$\{a,b\} \rightarrow \{c,d\}$ = The automorphism which takes a to c and b to d, here the automorphism is an element of a group of automorphisms.

Other notations, especially notations of number theory, have been used throughout the thesis, but these will present no difficulty since they are standard notations and they will be understood from the context.

3. Dihedral Group [1, p.89]*

Consider the groups of symmetries of a regular n sided polygon, call its vertices 0,1,2,..., n-1.

If one rotates the regular polygon through an angle of $\frac{2\pi}{n}$ about the line passing through the center and perpendicular to the plane of the polygon then

$$0 \rightarrow 1, \quad 1 \rightarrow 2, \quad \ldots, \quad n-1 \rightarrow 0 .$$

---

*[1, p.89] = Page 89 of the book whose number is 1 in the entries of the Bibliography. Here, and within the text hereafter, square brackets like this will have corresponding meaning.

But a rotation through an angle of $r.\frac{2\pi}{n}$, (where $r = 0,1,\ldots,n-1$) will cause the vertices to move as such

$$0 \to 0+r,\ 1 \to 1+r,\ \ldots,\ n-1 \to (n-1)+r = r-1 \qquad (n-1+r \equiv r-1 \pmod{n}$$

Therefore we may rotate the polygon through one of the following angles

$$0,\ \frac{2\pi}{n},\ 2.\frac{2\pi}{n},\ \ldots,\ (n-1).\frac{2\pi}{n}$$

These are n rotations and one may denote them by

$$e,\ b,\ b^2,\ \ldots,\ b^{n-1}$$

where b represents a rotation of $\frac{2\pi}{n}$ and $b^n = b^0 = e$. Obviously e is the identity operation since every vertex remains fixed.

The group of symmetries also contains reflections. If n is odd, all reflections are geometrically equivalent, the axis of reflection in each case being the line joining a vertex and the midpoint of the opposite side. There are n symmetries of this type. If n is even, however, they fall into two classes of $\frac{n}{2}$ reflections each, because an axis of symmetry through one vertex also contains the opposite one, and an axis through the midpoint of a side also passes through the opposite midpoint.

Actually a reflection is a rotation through an angle π about one of the mentioned axes. Let a represent a reflection; then obviously $a^2 = e$, since a^2 represents a double reflection or a rotation through 2π about an axis, which leaves every vertex fixed.

Considering a and its powers, b and its powers, then one will have $2n$ elements of the form $a^i b^j$ $(i = 0,1;\ j = 0,1,\ldots,n-1)$ that

will bring the polygon into itself. Considering the geometry of the polygon then one can see that $ba = ab^{-1}$ i.e. $a^{-1}ba = b^{-1}$. These $2n$ elements form a group generated by the two elements a and b, and its defining relations are

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

Since $a^{-1}ba = b^{-1}$ implies $(ab)^2 = e$, then the defining relations may be expressed in the form

$$a^2 = b^n = (ab)^2 = e .$$

The elements of this group are

$$[a^0b^0, a^0b, \ldots, a^0b^{n-1}, ab^0, ab, \ldots, ab^{n-1}]$$

or better yet

$$[e, b, \ldots, b^{n-1}, a, ab, \ldots ab^{n-1}].$$

One can write the elements of the group as b^ja^i, $(j = 0,1,\ldots,n-1;\ i = 0,1)$ since,

$$a^0b^j = b^ja^0 = b^j$$

and $ab^j = b^{-1}ab^{j-1}$ since $ba = ab^{-1}$ which means $ab = b^{-1}a$

$$= b^{-2}ab^{j-2}$$

$$\vdots$$

$$= b^{-j}ab^{j-j}$$

$$= b^{-j}a$$

$$= b^{n-j}a .$$

Now $(ab^j)^2 = e$,

because $(ab^j)^2 = (ab^j)(ab^j)$

$= ab^{j-1}\ ab^{-1}\ b^j$ since $ba = ab^{-1}$

$= ab^{j-2}\ ab^{-2}\ b^j$

$\vdots$

$= a^2\ b^{-j}\ b^j = e.$

Therefore $(ab^j)^2 = e$ for all j $(j = 0,1,\ldots,n-1)$.

The above group is called the dihedral group D_n. The elements b^j $(j = 0,1,\ldots,n-1)$ are the n rotations, and the elements ab^j $(j = 0,1,\ldots,n-1)$ are the n reflections.

Analytical expressions for the elements of D_n can be found as follows:

If x varies over the values $1,2,\ldots,n-1, n$ which denote the vertices of the regular polygon in counter-clockwise order, the rotation b is described by the congruence relation

$$x^b \equiv x + 1 \pmod{n} \qquad (1)$$

and in general $x^{b^j} \equiv x + j \pmod{n}$,

therefore $x^{b^n} \equiv x + n \pmod{n}$

which is an identity relation since

$$x + n \equiv x \pmod{n},$$

i.e. $b^n = e$.

Again, if $x = 1 + z$, the image of x under the reflection a is given by $x^a \equiv 1 - z$. Thus one has

$$x^a \equiv 2 - x \pmod{n} \qquad (2)$$

and

$$x^{a^2} \equiv (2 - (2-x)) \pmod{n}$$

which is an identity relation since $2 - (2-x) = x$. i.e. $a^2 \equiv e$.

All relations between the generating elements a and b may be derived from (1) and (2); e.g., one has

$$x^{ab} \equiv (x^a)^b \equiv (2-x)^b \equiv (2-x) + 1 = 3-x$$

and

$$x^{(ab)^2} \equiv 3 - (x^{ab}) \equiv 3 - (3-x) = x,$$

i.e.

$$(ab)^2 = e.$$

Therefore

$$a^2 = b^n = (ab)^2 = e.$$

4. Analogue Group

The defining relations of this group are

$$a^3 = b^n = (ab)^3 = e \ , \quad a^{-1} ba = b^k.$$

This analogue group G_n may describe a group of summetries in a space of higher dimension than that of D_n. This is because G_n has the element a of order 3 in contrast to that element a in D_n which is of order 2.

CHAPTER II

PROPERTIES OF THE DIHEDRAL GROUP

1. Existence

In the introduction, the group of symmetries of an n sided regular polygon was found to have the following defining relations:

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

When $n < 3$, these relations still define a group. However, the regular polygon is degenerate, and the group has no significance for the purpose of this thesis. Therefore, D_n will represent a group for $n > 2$, n being a positive integer.

2. The Center of D_n

It is a well known theorem [1, p.103] that, the aggregate of self-conjugate elements of a group G forms an Abelian group Z, which is called the center of G.

One now finds those elements of D_n that form the center Z of D_n.

Obviously $e \in Z$.

One may divide the elements of D_n, other than e, into two classes:

1) Those elements of the form ab^j $(0 \leq j \leq n-1)$

2) Those elements of the form b^j $(0 \leq j \leq n-1)$.

Elements of class (1) are not self-conjugate, since suppose ab^j is self-conjugate, i.e.

$$(ab^k)(ab^j) = (ab^j)(ab^k) , \qquad (0 \leq k \leq n-1)$$

then

$$(ab^j)^{-1}(ab^k)(ab^j) = (ab^k)$$

$$b^{-j}a^{-1}ab^kab^j = ab^k$$

$$b^{k-j}\, ab^j = ab^k ,$$

$$ab^{2j-k} = ab^k .$$

This implies that $b^{2(k-j)} = e$ and this in turn implies that $2k \equiv 2j \pmod{n}$ but both k and j are less than n. Therefore, $k = j$ unless n is even, when $k = j \pm \frac{n}{2}$ is possible. Hence ab^j commutes with ab^k only when one of these special relations exists between j and k. Therefore, no element ab^j is self-conjugate, and hence none of them belongs to Z.

Elements of class (2) form the cyclic subgroup b of D_n. Since b is cyclic then it is abelian and therefore b^j commutes with b^i for all j and i $(0 \leq j \leq n-1;\ 0 \leq i \leq n-1)$. There remains to check for elements of class (2) that commute with elements of class (1).

Suppose

$$b^j(ab^i) = (ab^i)\, b^j , \qquad (0 \leq i \leq n-1;\ 0 \leq j \leq n-1)$$

then

$$(ab^j)^{-1}\, b^j(ab^i) = b^j$$

$$b^{-i}\, a^{-1}\, b^j\, ab^i = b^j$$

$$b^{-i}\, ab^{j}\, ab^{i} = b^{j}, \qquad \text{since } a = a^{-1}$$

$$b^{-i}\, b^{n-j}\, a^{2} b^{i} = b^{j}, \qquad \text{since } ab^{j} = b^{-j}a = b^{n-j}a.$$

Therefore

$$b^{n-j} = b^{j}.$$

This equality holds if $n \equiv 2j \pmod{n}$, but $(0 \leq j \leq n-1)$, therefore $n = 2j$ and $j = \frac{n}{2}$, since j is an integer, therefore $j = \frac{n}{2}$ can hold only when n is even.

Hence, if n is odd, then Z is made up of one element only namely the identity element; and if n is even then Z is made up of two elements namely e and $b^{n/2}$. Clearly if n is even then $b^{n/2}$ is of order 2.

3. The Factor Group of D_n With Respect to its Center Z, i.e. $D_{n/Z}$

Applying the definition of the factor group [2, p.84], one can see clearly that when n is odd, then $D_{n/Z} \sim D_n$, and therefore $D_{n/Z}$ is a dihedral group.

When n is even, then Z is $[e, b^{n/2}]$. Since D_n is of order $2n$ and Z is of order 2, $D_{n/Z}$ is of order $\frac{2n}{2} = n$.

Now $$a^{i}\, b^{\frac{n}{2}+k} Z = a^{i} b^{k} Z, \qquad (i = 0,1;\ 0 \leq k \leq \tfrac{n}{2} - 1)$$

since $$a^{i}\, b^{\frac{n}{2}+k} Z = a^{i} b^{\frac{n}{2}+k} [e, b^{\frac{n}{2}}] = a^{i} b^{\frac{n}{2}+k},\ a^{i} b^{k}$$

and $$a^{i}\, b^{k} Z = a^{i}\, b^{k} [e, b^{\frac{n}{2}}] = a^{i} b^{k},\ a^{i} b^{\frac{n}{2}+k}.$$

One can easily show that the elements $a^i b^k Z$, $(i = 0,1;\ 0 \le k \le \frac{n}{2} - 1)$ are all distinct and their number is n. These elements form the elements of $D_{n/Z}$; they are

$$[Z,\ bZ,\ b^2Z,\ \ldots,\ b^{\frac{n}{2}-1}Z,\ aZ,\ abZ,\ \ldots,\ ab^{\frac{n}{2}-1}Z] .$$

Let $\alpha = aZ$ and $\beta = bZ$, then the defining relations of this group are $\alpha^2 = \beta^{\frac{n}{2}} = e$, $\alpha^{-1}\beta\alpha = \beta^{-1}$. Therefore this group is also a dihedral group.

Hence $D_{n/Z}$ is a dihedral group for all n.

4. The Commutator Subgroup C of D_n

If a and b are any two elements of a group G, then the commutator C_i of a and b is defined as: $a^{-1}b^{-1}ab$. If a and b run independently through the whole group, one obtains the commutators $C_1, C_2, \ldots, C_m$. It is possible that the product of two commutators cannot itself be written as a commutator. But in any case the set of all commutators generates a certain group $C = \{C_1, C_2, \ldots, C_m\}$ which is called the commutator subgroup or commutator group of G [1, p.104].

Consider ab^k and ab^j of D_n, $(0 \le k \le n-1\ ;\ 0 \le j \le n-1)$ then

$$(ab^k)^{-1}(ab^j)^{-1}(ab^k)(ab^j) = b^{-k}\, a^{-1}\, b^{-j}\, a^{-1}\, ab^k\, ab^j$$

$$= b^{-k}\, ab^{k-j}\, ab^j, \quad \text{since } a^{-1}a = e$$

$$= ab^{2k-j}\, ab^j, \quad \text{since } b^{-k}\, a = ab^k$$

$$= a^2\, b^{2(j-k)}, \quad \text{since } b^{-k}\, a = ab^k$$

$$= b^{2(j-k)}, \quad \text{since } a^2 = e.$$

Therefore all commutators of elements of the form ab^j $(0 \leq j \leq n-1)$ are of the form b^{2i}, i being an integer, i.e. they are even powers of b (mod n).

Again, consider b^k and b^j of D_n, $(0 \leq k \leq n-1 \; ; \; 0 \leq j \leq n-1)$ then

$$b^{-k} b^{-j} b^k b^j = b^0 = e ,$$

for all k and j.

Therefore, elements of the form b^j $(0 \leq j \leq n-1)$ will form only one commutator namely the identity.

There remains to form commutators of elements of the form b^j $(0 \leq j \leq n-1)$ and elements of the form ab^k $(0 \leq k \leq n-1)$ by taking one from each set, and one has

$$b^{-j}(ab^k)^{-1} b^j(ab^k) = b^{-j} b^{-k} a^{-1} b^j ab^k$$

$$= b^{-(j+k)} a^{-1} ab^{k-j} , \text{ since } b^j a = ab^{-j}$$

$$= b^{-2j}.$$

Therefore all commutators of this type are also elements of even powers of b (mod n).

There always exists the following commutator:

$$a^{-1} b^{-1} ab = a^2 b^2 = b^2.$$

Consider the cyclic group $\{b^2\}$. If n is even then $\{b^2\}$ is a subgroup of $\{b\}$ and the elements of $\{b^2\}$ are the elements that are even powers of b in $\{b\}$, and the order of this subgroup is clearly $\frac{n}{2}$. This group is the commutator subgroup C of D_n, since all commutators are of even powers of b (mod n).

Again, consider the cyclic group $\{b^2\}$ when n is odd. Then $\{b^2\} = \{b\}$, since $(2,n) = 1$. This group is the commutator subgroup C of D_n, since all commutators are even powers of b (mod n).

Hence, whether n is odd or even, the commutator subgroup C of D_n is $\{b^2\}$.

5. The Factor Group of D_n With Respect to the Commutator Subgroup C

It was shown in the previous section that C is $\{b^2\}$.

The factor group D_n/C is of order 2 when n is odd, because here C is of order n and therefore D_n/C is of order $\frac{2n}{n} = 2$. When n is even then C is of order $\frac{n}{2}$ and D_n/C is of order $\frac{2n}{n/2} = 4$.

When n is odd then $D_n/C = [C, aC]$ which is cyclic.

When n is even then $D_n/C = [C, aC, bC, abC]$ and this is the four group (the non-cyclic group of order 4).

6. Sylow Subgroups of D_n

One of the fundamental theorems in the theory of finite groups is the following [2, p.58]:

Let G be a group of order n and let p^α be the highest power of a prime p contained in n as a factor, α being a positive integer. Then G contains at least one subgroup of order p^α. All its subgroups of order p^α form a single complete conjugate set, and their number is $1 + kp$, where k is non-negative integer. Such a subgroup of order p^α is called a Sylow subgroup.

(i) Let n be odd in D_n, then the order of D_n is $2n = 2 \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $p_i \neq p_j$ for $i \neq j$ and p_i is an odd prime $(1 \leq i \leq k \; ; \; 1 \leq j \leq k)$.

Applying the theorem, one concludes that there exists a Sylow subgroup of order 2. In fact there are n Sylow subgroups of order 2, and this is because there are n elements of the form ab^j $(0 \leq j \leq n-1)$ that are of order 2. Clearly they are all cyclic.

There exists one, and only one, Sylow subgroup S_i of order $p_i^{\alpha_i}$ for each i $(1 \leq i \leq k)$, and they are all cyclic. This is because, $p_i^{\alpha_i}$ is an odd number and therefore all the elements of S_i are of odd order, hence S_i is a subgroup of $\{b\}$. But $\{b\}$ is cyclic, therefore the result follows immediately by applying the theorem [1, p.38] which states: "All subgroups of a cyclic group are cyclic. If $\{b\}$ is a cyclic group of order g, then corresponding to every divisor h of g there exists one, and only one, subgroup of order h, which may be generated by $b^{g/h}$".

Therefore when n is odd then all Sylow subgroups of D_n are cyclic.

(ii) When n is even then there may exist Sylow subgroups that are not cyclic, e.g. if $2n = 2^2 \prod_{i=1}^{k} p_i^{\alpha_i}$, p_i is an odd prime for all i, then there exist $\frac{n}{2}$ Sylow subgroups of order 4 which are isomorphic to the four group .

7. The Group of Automorphisms of the Dihedral Group; $A(D_n)$

a) It was shown that D_n is generated by a and b i.e. $D_n = \{a,b\}$ where $a^2 = b^n = e$, $a^{-1} ba = b^{-1}$.

The number of ways by which D_n can be represented by $\{c,d\}$ where $c^2 = d^n = e$, $c^{-1} dc = d^{-1}$ i.e. the number of sets of generators is the order of $A(D_n)$.

It was shown earlier that every element of the form ab^j $(0 \leq j \leq n-1)$ is of order 2. There are n of these elements.

Every element of order n must be of the form b^i where $(n,i) = 1$, $(0 \leq i \leq n-1)$. There are $Q(n)$ elements of order n, where Q is the Euler Q-function.

There may exist elements of the form b^k of order 2, but these are generated by b^i. Therefore $D_n \neq \{b^k, b^i\}$ and hence D_n can only be generated by sets of the form $\{ab^j, b^i\}$, $(n,i) = 1$. Furthermore this always works, because

1) b^i generated b.

2) ab^j and b^i generate a, since b^i generates b^{-j} and $D_n = \{a,b\}$.

Since ab^j may be chosen in n ways, and b^i in $Q(n)$ ways, therefore the order of $A(D_n)$ is $n.Q(n)$.

Since $Q(n) = n \prod_{p|n} (1 - \frac{1}{p})$, [4, p.29], where the notation indicates a product over all the distinct primes which divide n, then applying this one can show easily that $Q(n)$ is even for all positive integers $n > 2$. Hence $n \cdot Q(n)$ is always even.

b) The following is a well known theorem on inner automorphisms [3, p.85]; "The inner automorphisms of a group G form a normal subgroup $I(G)$ of the group $A(G)$ of all automorphisms of G. Also the mapping $a \rightarrow Aa$ (where $a \in G$ and $Aa \in I(G)$) is a homomorphism of G onto $I(G)$ whose kernel is the center of G." Therefore $I(G) \sim G/Z$.

Consequently, $I(D) \sim D_n/Z$. It was shown that when n is odd then $Z = e$, and hence, $I(D) \sim D_n/Z = D_n$ i.e. $I(D_n)$ is a dihedral group of order $2n$. When n is even then $I(D_n) \sim D_n/Z$ and therefore $I(D_n)$ is a dihedral group of order n, since D_n/Z is a dihedral group of order n as was shown.

Clearly a dihedral group is not abelian, therefore $I(D_n)$ is not abelian and this in turn implies that $A(D_n)$ is not abelian.

c) The elements of $A(D_n)$ can be written as follows:

$$\alpha_{ij} = \{a,b\} \longrightarrow \{ab^i, b^j\} ,$$

where $(i = 0,1,\ldots, n-1)$ and $(j,n) = 1$, $j < n$.

Consider the element

$$\alpha : \{a,b\} \longrightarrow \{a, b^{-1}\} \quad \text{i.e.} \quad ab^j \rightarrow ab^{-j}$$

then

$$a^{-1}\, ab^j\, a = b^j a = ab^{-j}$$

and hence α is an inner automorphism. Consider the element

$$\beta_2 = \{a,b\} \longrightarrow \{ab^2, b\} \quad \text{i.e.} \quad ab^j \rightarrow ab^{j+2} ,$$

then

$$b^{-1}\, ab^{j} b = ab^{j+2}$$

and hence β_2 is an inner automorphism. Now

$$\alpha\beta_2 = \{a,b\} \xrightarrow{\alpha} \{a,b^{-1}\} \xrightarrow{\beta_2} \{ab^2,\, b^{-1}\} = \{a,b\} \to \{ab^2, b^{-1}\}.$$

Obviously this $\alpha\beta_2$ is also inner since it is the product of two inner automorphisms.

$$\alpha^2 = \{a,b\} \xrightarrow{\alpha} \{a,b^{-1}\} \xrightarrow{\alpha} \{a,b\} = \{a,b\} \to \{a,b\}\ ,$$

i.e. α is of order 2.

When n is even, let $n = 2m$, then

$$(\beta_2)^1 = \{a,b\} \to \{ab^2,\, b\}$$

$$(\beta_2)^2 = \{a,b\} \to \{ab^4,\, b\}$$

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

$$(\beta_2)^m = \{a,b\} \to \{ab^{2m},\, b\}$$

$$= \{a,b\} \to \{a,\, b\}$$

i.e. β_2 is of order $m = \frac{n}{2}$.

When n is odd, let $n = 2m+1$, then

$$(\beta_2)^1 = \{a,b\} \to \{ab^2,\, b\}$$

$$(\beta_2)^2 = \{a,b\} \to \{ab^4,\, b\}$$

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

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

$$(\beta_2)^m = \{a, b\} \longrightarrow \{ab^{2m}, b\}$$

$$(\beta_2)^{m+1} = \{a, b\} \longrightarrow \{ab^{(2m+1)+1}, b\}$$

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

$$(\beta_2)^{m+i} = \{a, b\} \longrightarrow \{ab^{(2m+1)+2i-1}, b\} \quad , \qquad i < m$$

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

$$(\beta_2)^{2m} = \{a,b\} \longrightarrow \{ab^{(2m+1)+2m-1}, b\}$$

$$(\beta_2)^{2m+1} = \{a, b\} \longrightarrow \{ab^{(2m+1)+2m+1}, b\}$$

$$= \{a, b\} \longrightarrow \{a, b\}$$

i.e. β_2 is of order $2m+1 = n$.

Now
$$(\alpha\beta_2)^2 = \{a, b\} \xrightarrow{\alpha\beta 2} \{ab^2, b^{-1}\} \xrightarrow{\alpha\beta_2} \{ab^2\, b^{-2}, b\}$$

$$= \{a, b\} \longrightarrow \{a, b\} \ ,$$

i.e. $\alpha\beta_2$ is of order 2.

Now, when n is even, then $H_1 = \{\alpha, \beta_2\}$ whose defining relations are

$$\alpha^2 = \beta_2^{n/2} = e, \quad \alpha^{-1} \beta_2 \alpha = \beta_2^{-1} \ ,$$

and this H_1 is $I(D_n)$.

When n is odd, then $H_2 = \{\alpha, \beta_2\}$ whose defining relations are

$$\alpha^2 = \beta_2^n = e \ , \quad \alpha^{-1} \beta_2 a = \beta_2^{-1} \ ,$$

and this H_2 is $I(D_n)$.

Now, consider the following automorphisms:

$$\alpha = \{a, b\} \longrightarrow \{a, b^{-1}\}$$

which was shown to be inner and of order 2.

$$\beta = \{a, b\} \longrightarrow \{ab, b\}$$

this is obviously of order n, whether n is odd or even.

$$\alpha\beta = \{a, b\} \xrightarrow{\alpha} \{a, b^{-1}\} \xrightarrow{\beta} \{ab, b^{-1}\} = \{a, b\} \longrightarrow \{ab, b^{-1}\}$$

$$(\alpha\beta)^2 = \{a, b\} \xrightarrow{\alpha\beta} \{ab, b^{-1}\} \xrightarrow{\alpha\beta} \{abb^{-1}, b\} = \{a, b\} \longrightarrow \{a, b\}$$

i.e. $\alpha\beta$ is of order 2, therefore

$$H_3 = \{\alpha, \beta\}$$

is a dihedral group of order 2n, since

$$\alpha^2 = \beta^n = e \quad \text{and} \quad \alpha^{-1}\beta\alpha = \beta^{-1}$$

when n is odd then β is inner, since it can be generated by the inner automorphism β_2, $\beta_2^{m+1} = \beta$. Therefore $H_3 = H_2$. When n is even then β is not inner for the simple reason that $H_3 \neq H_1$, since H_1 is $I(D_n)$ and is of order n, while H_3 is of order 2n.

More generally one may consider the automorphism

$$\beta_i = \{a, b\} \longrightarrow \{ab^i, b\},$$

where $(i, n) = 1$, then

$$(\beta_i)^k = \{a, b\} \longrightarrow \{ab^{ki}, b\},$$

and since

$$k_i \not\equiv n \pmod{n}\ ,\quad (i, n) = 1 \quad \text{for all} \quad 0 < k < n$$

and

$$k_i \equiv n \pmod{n}\ ,\quad (i, n) = 1 \quad \text{when} \quad k = n \quad \text{or} \quad k = nl$$

and hence β_i is of order n, $(i, n) = 1$.

$$(\alpha\beta_i) = \{a, b\} \xrightarrow{\alpha} \{a, b^{-1}\} \xrightarrow{\beta_i} \{ab^i, b^{-1}\}$$

and

$$(\alpha\beta_i)^2 = \{a, b\} \xrightarrow{\alpha\beta_i} \{ab^i, b^{-1}\} \longrightarrow \{ab^ib^{-i}, b\}$$

$$= \{a, b\} \longrightarrow \{a, b\} \quad \text{i.e.} \quad \alpha\beta_i \quad \text{is of order 2.}$$

Therefore $H_i = \{\alpha, \beta_i\}$ is also a dihedral group of order $2n$. In fact $H_i = H_3$ since β generates β_i.

Still more generally, when one considers the automorphism

$$\beta_j = \{a, b\} \longrightarrow \{ab^j, b\}\ ,\quad (j, n) = d_j$$

$$(\beta_j)^k = \{a, b\} \longrightarrow \{ab^{kj}, b\} = \{a, b\} \longrightarrow \{a, b\}\ ,\quad \text{when} \quad kj \equiv n \pmod{n}.$$

Let $j = d_j\mathfrak{j}$ and $n = d_jm$ then $kj = kd_j\mathfrak{j}$ and hence $k\mathfrak{j} \equiv m \pmod{n}$ but $(\mathfrak{j}, m) = 1$ i.e. $k = m$ or $k = cm$, and here $k = m = \frac{n}{d_j}$ is the least positive integer that will do, therefore β_j is of order $\frac{n}{d_j}$. Here also the group $H_j = \{\alpha, \beta_j\}$ is a dihedral group of order $\frac{2n}{d_j}$.

CHAPTER III

PROPERTIES OF THE ANALOGUE GROUP

1. Existence

a) If the following defining relations are given

$$a^3 = b^n = (ab)^3 = e, \qquad a^{-1} ba = b^k$$

then these defining relations will define a group provided

$$k^2 + k + 1 \equiv 0 \pmod{n}$$

since

$$a^{-1} ba = b^k \longrightarrow ba = ab^k$$

and

$$e = (ab)^3 = ab\ ab\ ab = a^2b^{k+1}\ ab = a^3b^{(k+1)k+1} = a^3b^{k^2+k+1}$$

therefore

$$k^2 + k + 1 \equiv 0 \pmod{n} .$$

Since $k^2 + k + 1 \equiv 0 \pmod{n}$, then obviously n is odd always, and moreover $nm = k^2 + k + 1$ implies $(k, mn) = 1$ and hence $(k,n) = 1$, m and n being positive integers.

b) The group defined as shown above will be called here: "The Analogue Group G_n". This group is of order $3n$ and its elements

are given by $a^i b^j$ [$i \equiv 0,1,2 \pmod 3$; $j \equiv 0,1,\ldots,n-1 \pmod n$]. The group $\{b\}$ is a cyclic subgroup of G_n. The rest of the elements are all of order 3, since

$$(a^i b^j)^3 = a^i b^j \, a^i b^j \, a^i b^j , \qquad (i = 1,2; \; j = 0,1,\ldots,n-1)$$

$$= a^{2i} b^{jk^i + j} \, a^i b^j , \qquad \text{since } ba = ab^k \text{ and } ba^i = a^i b^{k^i}$$

$$= a^{3i} b^{(jk^i + j)k^i + j}$$

$$= b^{j(k^{2i} + k^i + 1)}$$

$$= e .$$

The last step namely $b^{j(k^{2i}+k^i+1)} = e$ is valid because,

$$k^{2i} + k^i + 1 = k^2 + k + 1 \equiv 0 \pmod n, \qquad i = 1$$

and $k^{2i} + k^i + 1 = k^4 + k^2 + 1 = (k^2 + k + 1)(k^2 - k + 1) \equiv 0 \pmod n$, $i = 2$.

Clearly

$$a^{-1} = a^2 \text{ and } (b^j)^{-1} = b^{-j} = b^{n-j} , \qquad (j = 0,1,\ldots,n-1)$$

and

$$(ab^j)^{-1} = b^{-j} a^{-1} = b^{-j} a^2 = ab^{-jk} a = a^2 b^{-jk^2}$$

$$(a^2 b^j)^{-1} = b^{-j} a^{-2} = b^{-j} a = ab^{-jk} .$$

An interesting special case is when $k = 1$, then

$$k^2 + k + 1 = 3,$$

and

$$a^3 = b^3 = (ab)^3 = e, \quad a^{-1} b a = b$$

will define an abelian group of order $3 \cdot 3 = 9$ and all the elements are of order 3 except the identity. Hereafter, the thesis will be concerned with $k > 1$.

c) Upon replacing k by k^2 in $k^2 + k + 1 \equiv 0 \pmod{n}$, one has

$$k^4 + k^2 + 1 \equiv 0 \pmod{n} \quad \text{and} \quad (k^2, n) = 1 .$$

Furthermore

$$k^2 \not\equiv k \pmod{n},$$

because, suppose

$$k^2 \equiv k \pmod{n}$$

then

$$k(k-1) \equiv 0 \pmod{n}.$$

Since $(k,n) = 1$, it follows that $n \mid (k-1)$, but this is impossible because $k < n$. Therefore k and k^2 are distinct modulo n. Now

$$k^4 + k^2 + 1 \equiv k^2 + k + 1 \pmod{n}$$

therefore

$$k^4 \equiv k \pmod{n}.$$

One may also note that $k^3 \equiv 1 \pmod{n}$, because $k^3 - 1 = (k-1)(k^2+k+1)$.

d) From the discussion above one concludes that corresponding to every n, for which an analogue group G_n is defined, there exist at least two distinct numbers (modulo n) namely k and k^2.

Let G_n have the following defining relations

$$a^3 = b^n = (ab)^3 = e, \qquad a^{-1} ba = b^k$$

and let G_n' have the defining relations

$$c^3 = d^n = (cd)^3 = e, \qquad c^{-1} dc = d^{k^2} ,$$

then $G_n \sim G_n'$, and the isomorphism is established by the correspondence

$$a \rightarrow c^2$$

$$b \rightarrow d ,$$

and to prove the isomorphism, one has

$$a^i b^j \rightarrow c^{-i} d^j \qquad , \qquad (i = 0,1,2; \quad j = 0,1,\ldots,n-1)$$

$$a^p b^q \rightarrow c^{-p} d^q \qquad , \qquad (p = 0,1,2; \quad q = 0,1,\ldots,n-1)$$

$$a^i b^j \cdot a^p b^q = a^{(i+p)} b^{jk^p+2}$$

$$a^{(i+p)} b^{jk^p+q} \rightarrow c^{-(i+p)} d^{jk^p+q} ,$$

but

$$c^{-i} d^j c^{-p} d^q = c^{-(i+p)} d^{j(k^2)^{-p}+q} = c^{-(i+p)} d^{jk^p+q} ,$$

the last equality holds, since $-p \equiv 2p \pmod 3$ and $k^4 \equiv k \pmod n$ i.e.

$$c^{-(i+p)} d^{j(k^2)^{-p}+q} = c^{-(i+p)} d^{j(k^2)^{2p}+q} = c^{-(i+p)} d^{jk^p+q} .$$

Therefore isomorphism is established.

The set k and k^2 is not unique for every n, since when $n = 91$ one has

$$k_1 = 9 , \qquad k_1^2 = 81$$

and

$$k_2 = 16, \qquad k_2^2 = 74 .$$

It was shown above that k_1 and k_1^2 give the same analogue group. Obviously k_2 and k_2^2 will also give the same analogue group. The question now is whether k_1 and k_2 will give the same group, and the answer is negative. Suppose that k_1 and k_2 satisfy the following

$$k_1^2 + k_1 + 1 \equiv 0 \pmod{n}$$

$$k_2^2 + k_2 + 1 \equiv 0 \pmod{n}$$

$$k_1 \not\equiv k_2$$

and

$$k_1^2 \not\equiv k_2 \pmod{n}.$$

Let $(G_n)_1$ have the defining relations

$$a^3 = b^n = (ab)^3 = e, \quad a^{-1} ba = b^{k_1} ;$$

and let $(G_n)_2$ have the defining relations

$$c^3 = d^n = (cd)^3 = e, \quad c^{-1} dc = d^{k_2} .$$

Then both $(G_n)_1$ and $(G_n)_2$ are analogue groups of the same order $3n$; but they are not isomorphic, because trying all possible ways of isomorphism between them will fail, and this can be shown as follows:

In any isomorphism one must have a correspondence of generators of the form

$$\{a,b\} \rightarrow \{c^i d^j, d^p\} \quad (i \equiv 1,2 \bmod 3 \ ; \ (p,n) = 1).$$

Now

$$a^{-1}\ ba \longrightarrow (c^i d^j)^{-1}\ d^p\ (c^i d^j) = d^{pk_2^i}$$

and

$$b^{k_1} \longrightarrow d^{pk_1}\ .$$

Since

$$a^{-1}\ ba = b^{k_1},$$

one has

$$pk_1 \equiv pk_2^i \pmod{n}$$

$$k_1 \equiv k_2^i \pmod{n} \quad \text{because} \quad (p,n) = 1\ ,$$

therefore

$$k_1 = k_2 \quad \text{or} \quad k_2^2 \quad \text{because} \quad i = 1 \text{ or } 2.$$

But this contradicts the hypothesis.

If $3^\alpha | n$ then $\alpha = 1$, because

$$(k^i)^2 + k^i + 1 = (k^i - 1)^2 + 3(k^i - 1) + 3 \equiv 0 \pmod{n}, \quad (i = 1,2)$$

and this implies that $(k^i - 1, n) = 1$ or 3, and if $(k^i - 1, n) = 3$, then

$$\frac{(k^i - 1)^2}{3} + (k^i - 1) + 1 \equiv 0 \pmod{\frac{n}{3}}\ ,$$

now if $3 | (\frac{n}{3})$ then

$$3 | (\frac{(k^i - 1)^2}{3} + (k^i - 1) + 1),$$

but

$$3 | (\frac{(k^i - 1)^2}{3} + (k^i - 1),$$

therefore $3 | 1$ which is impossible, and hence $3 \nmid \frac{n}{3}$ i.e. if $3^\alpha | n$ then $\alpha = 1$.

2. The Center of G_n

Let the center of G_n be denoted by Z.

One may divide the elements of G_n into two classes:

(1) Those elements of the form $a^i b^j$, $(i = 1,2;\ j = 0,1,\ldots,n-1)$

(2) Those elements of the form b^j, $(j = 0,1,\ldots,n-1)$.

None of the elements in class (1) belongs to Z, since

$$a^{-1}a^i b^j a = a^i b^{jk},$$

therefore

$$a^i b^j \notin Z, \quad (i = 1,2;\ j = 0,1,\ldots,n-1).$$

Elements of class (2) have the element $b^0 = e \in Z$. As for the rest of the elements in this class, i.e. b^j $(j = 1,2,\ldots,n-1)$, one may note that $\{b\}$ is a cyclic subgroup of G_n and therefore b^j commutes with b^p for all j and p $(j = 0,1,\ldots,n-1;\ p = 0,1,\ldots,n-1)$. There remains to determine those elements of class (2) that commute with elements of class (1). Then

$$(a^i b^p)^{-1} b^j (a^i b^p) = b^{-p} a^{-i} b^j a^i b^p, \quad (i = 1,2;\ j = 1,\ldots,n-1;\ p = 0,1,\ldots,n-1)$$

$$= b^{-p+jk^i+p}$$

$$= b^{jk^i}.$$

Therefore b^j will be self-conjugate provided $jk^i \equiv j \pmod n$, but $k^i \not\equiv 1 \pmod n$, therefore $jk^i \equiv j \pmod n$ implies $(j,n) \neq 1$. It was shown earlier that $(k^i-1,n) = 1$ or 3, and now $jk^i \equiv j \pmod n$ implies

$j(k^i-1) \equiv 0 \pmod{n}$. Therefore,

(i) If $(k^i-1,n) = 1$ then $j = qn$ but $j < n$ and hence $b^j \notin Z$ and this is the case when $3 \nmid n$.

(ii) If $(k^i-1,n) = 3$ then $j = q\frac{n}{3}$, $j < n$ and therefore if $q = 1$ or 2 then $b^{n/3} \in Z$ and $b^{2n/3} \in Z$. This is the case when $3|n$.

In conclusion,

$$Z = [e], \quad \text{when} \quad 3 \nmid n$$

and

$$Z = [e, b^{\frac{n}{3}}, b^{\frac{2n}{3}}], \quad \text{when} \quad 3|n.$$

The analogy with the center of D_n is obvious.

3. The Factor Group $G_{n/Z}$

It was shown that when $3 \nmid n$ then $Z = [e]$ and therefore $G_{n/Z} \sim G_n$ and hence the order of $G_{n/Z} = 3n$.

When $3|n$ then, as was shown above, $Z = [e, b^{\frac{n}{3}}, b^{\frac{2n}{3}}]$ and therefore $G_{n/Z}$ is of order $\frac{3n}{3} = n$, and one has

$$a^i b^{\frac{2n}{3}+p} Z = a^i b^{\frac{n}{3}+p} Z = a^i b^p Z, \quad (i=0,1,2;\ p=0,1,\ldots,\tfrac{n}{3}-1),$$

since $b^{\frac{n}{3}}$ and $b^{\frac{2n}{3}}$ are in Z.

One can easily show that the elements $a^i b^p Z$, for all i and p, are all distinct and their number is n. These are the elements of $G_{n/Z}$.

Let $\alpha = aZ$ and $\beta = bZ$, then the defining relations of $G_{n/Z}$ are

$$\alpha^3 = \beta^{\frac{n}{3}} = (\alpha\beta)^3 = e, \quad \alpha^{-1}\beta\alpha = \beta^k .$$

Therefore this group is also an analogue group of order n. The analogy with $D_{n/Z}$ is also obvious.

4. The Commutator Subgroup C of G_n

Consider the commutator

$$(a^i b^j)^{-1}(a^s b^r)^{-1}(a^i b^j)(a^s b^r),$$

where $i = 0,1,2$; $s = 0,1,2$; $j = 0,1,\ldots,n-1$; $r = 0,1,\ldots,n-1$).
The given commutator reduces to

$$b^{j(k^s-1)-r(k^i-1)},$$

and the expression

$$j(k^s-1)-r(k^i-1)$$

is easily shown to have the factor $k-1$, whether i and s are $0,1$, or 2. Hence every commutator is a power of b^{k-1}; note that when $i = s = 0$ then one has $b^{-j}b^{-r}b^{j}b^{r} = e$ for all j and r. In particular, when $i = r = 0$ and $j = s = 1$, the commutator is b^{k-1} and this commutator generates the commutator subgroup C of G_n which is the cyclic subgroup $\{b^{k-1}\}$.

It was shown in section (1) of this chapter that, when $3 \nmid n$ then $(k-1,n) = 1$, and hence b^{k-1} is of order n and the commutator

subgroup $\{b^{k-1}\} = \{b\}$ which is of order n. When $3|n$, then $(k-1,n) = 3$ and hence b^{k-1} is of order $\frac{n}{3}$ and the commutator subgroup $\{b^{k-1}\}$ is a subgroup of $\{b\}$ and it is of order $\frac{n}{3}$. Here again the analogy is clear.

5. The Factor Group G_n/C

It was shown in the previous section that C is $\{b^{k-1}\}$ and that it is of order n, when $3 \nmid n$, and of order $\frac{n}{3}$ when $3|n$. Hence, the factor group G_n/C is of order 3 in the first case and is of order 9 in the second case. The elements of G_n/C, when $3 \nmid n$, are $[C, aC, a^2C]$ and this is the cyclic group $\{aC\}$ which is of order 3. The elements of G_n/C, when $3|n$, are

$$a^i b^j C \ (i \equiv 0,1,2 \pmod 3; \ j \equiv 0, \tfrac{n}{3}, \tfrac{2n}{3} \pmod n).$$

This group is generated by aC and $b^{\frac{n}{3}}C$, where both elements are of order 3, and it is an abelian group of order 9 in which all elements except the identity are of order 3. In fact it is the abelian analogue of order 9.

6. Sylow Subgroups of G_n [2,p.58]

(i) Let n be such that $3 \nmid n$, then the order of G_n is $3n = 3.\ p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, $p_i \neq p_j$ for $i \neq j$ and p_i is an odd prime $(1 \leq i \leq m; \ 1 \leq j \leq m)$.

Applying Sylow's theorem [2, p.58], one concludes that there exists a Sylow subgroup of order 3. In fact there are n Sylow

subgroups of order 3, and this is because there are n elements of the form ab^j $(j = 0,1,\ldots,n-1)$ and n elements of the form a^2b^j $(j = 0,1,\ldots,n-1)$ and every element of these is of order 3. Clearly these subgroups are all cyclic.

There exists one, and only one, Sylow subgroup S_i of order $p_i^{\alpha_i}$ for each i $(1 \leq i \leq m)$, because they are subgroups of the cyclic group $\{b\}$, and obviously all are cyclic.

Consequently, when $3 \nmid n$ then all Sylow subgroups of G_n are cyclic.

(ii) When n is such that $3|n$, then there exist Sylow subgroups that are not cyclic, since $3n = 3^2 \cdot p_1^{\alpha_1} \ldots p_m^{\alpha_m}$, where p_i is an odd prime for all i $(1 \leq i \leq m)$. In fact there exist $\frac{n}{3}$ Sylow subgroups of order 9 and these are abelian but not cyclic; all the elements are of order 3 except the identity.

7. The Group of Automorphisms of the Analogue Group; $A(G_n)$

It was shown that $G_n = \{a,b\}$ where $a^3 = b^n = (ab)^3 = e$, $a^{-1}ba = b^k$ and provided that $k^2 + k + 1 \equiv 0 \pmod{n}$.

The number of ways in which G_n can be represented by $\{c,d\}$, where $c^3 = d^n = (cd)^3 = e$, $a^{-1}ba = b^k$ and $k^2 + k + 1 \equiv 0 \pmod{n}$, i.e., the number of sets of generators, is the order of $A(G_n)$.

It was shown earlier that every element of the form a^ib^j $(i = 1,2;\ j = 0,1,\ldots,n-1)$ is of order 3. There are 2n of these elements.

Every element of order n must be of the form b^p where $(n,p) = 1$ and $(0 \leq p \leq n-1)$. There are $Q(n)$ elements of order n, where Q is the Euler Q-function.

There may exist elements of the form b^j of order 3, but these are generated by b^p. Therefore $G_n \neq \{b^j, b^p\}$ and hence G_n can only be generated by sets of the form $\{a^i b^j, b^p\}$, $(n,p) = 1$. Furthermore this always works, because

(1) b^p generates b

(2) $a^i b^j$ and b^p generate a.

Since $a^i b^j$ may be chosen in $2n$ ways, and b^p in $Q(n)$ ways, therefore the order of $A(G_n)$ is $2n\,Q(n)$. Since $n > 2$, therefore $Q(n)$ is even and $2n\,Q(n)$ always has 4 as a factor and one may express the order of $A(G_n)$ as $2n\,Q(n) = 2^i m$, $i \geq 2$ and m is odd.

(b) The group of inner automorphisms is isomorphic to the factor group with respect to the center, i.e. $I(G_n) \sim G_{n/Z}$. It was shown that when $3 \nmid n$ then $G_{n/Z}$ is an analogue group of order $3n$ and therefore $I(G_n)$, $3 \nmid n$, is also an analogue group of order $3n$. When $3 \mid n$ then $G_{n/Z}$ was shown to be an analogue group of order n and hence $I(G_n)$ for this case is also an analogue group of order n. Clearly an analogue group is non-abelian and hence $I(G_n)$ is non-abelian, and this in turn implies that $A(G_n)$ is also non-abelian.

Since $I(G_n)$ is a subgroup of $A(G_n)$, the order of $I(G_n)$ is a factor of the order of $A(G_n)$. Now,

(i) When $3|n$ then $I(G_n)$ is of order n and hence $n|2n\,Q(n)$ which is obviously true.

(ii) When $3 \nmid n$ then $I(G_n)$ is of order $3n$ and hence $3n|2n\,Q(n)$ and this implies that $3|Q(n)$. From this one concludes that n cannot be of the form p^{α} where $p = 6t + 5$ (p being a prime), and n cannot be of the form $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ where all the p's are of the form $6t + 5$ (p_i being a prime, for all i, $1 \leq i \leq m$), since $Q(n) = n \prod_{p_i|n} (1 - \frac{1}{p_i})$ and $1 - \frac{1}{p_i} = \frac{p_i - 1}{p_i}$, here $3 \nmid (p-1)$ for all i and $3 \nmid n$ and therefore $3 \nmid Q(n)$.

(c) The elements of $A(G_n)$ can be written as follows:

$$\alpha_{ijp} = \{a,b\} \longrightarrow \{a^i b^j,\ b^p\},$$

where $(i = 1,2)$; $(j = 0,1,\dots,n-1)$; and $(p,n) = 1$. This means that $a \rightarrow a^i b^j$ and $b \rightarrow b^p$ under $A(G_n)$, which is then completely determined because a and b generate G_n. Consider the element of $A(G_n)$

$$\alpha = \{a,b\} \longrightarrow \{a,b^k\}, \quad k \text{ is such that } k^2 + k + 1 \equiv 0 \pmod{n}.$$

It is noted that

$$a^{-1}\, a\, a = a$$
$$a^{-1}\, b\, a = b^k,$$

and therefore α is an inner automorphism. Now consider,

$$\beta = \{a,b\} \longrightarrow \{ab^{k-1},b\}, \quad k \text{ is such that } k^2 + k + 1 \equiv 0 \pmod{n}.$$

Then

$$bab^{-1} = ab^{k-1}$$

$$bb^{j}b^{-1} = b^{j}$$

and therefore β is an inner automorphism. Since α and β are inner then

$$\alpha\beta = \{a,b\} \rightarrow \{ab^{k-1},b^{k}\}$$

is also inner. Now,

$$\alpha^{2} = \{a,b\} \rightarrow \{a,b^{k^{2}}\} ,$$

$$\alpha^{3} = \{a,b\} \rightarrow \{a,b^{k^{3}}\} ,$$

$$= \{a,b\} \rightarrow \{a,b\} \quad , \qquad \text{since } k^{3} \equiv 1 \pmod{n},$$

and therefore α is of order 3.

Now

$$\beta^{2} = \{a,b\} \rightarrow \{ab^{2(k-1)},b\} ,$$

$$\beta^{3} = \{a,b\} \rightarrow \{ab^{3(k-1)},b\} ,$$

$$\vdots$$

$$\beta^{j} = \{a,b\} \rightarrow \{ab^{j(k-1)},b\} ;$$

and here if $(k-1,n) = 1$ then $j = n$, and hence β is of order n; but if $(k-1,n) = 3$ then $j = \frac{n}{3}$, hence β is of order $\frac{n}{3}$.

$$(\alpha\beta)^{2} = \{a,b\} \rightarrow \{ab^{k-1+k(k-1)},b^{k^{2}}\}$$

$$= \{a,b\} \rightarrow \{ab^{k^{2}-1},b^{k^{2}}\}$$

$$(\alpha\beta)^{3} = \{a,b\} \rightarrow \{ab^{k-1+k(k^{2}-1)},b^{k^{3}}\}$$

$$= \{a,b\} \rightarrow \{a,b\} \quad \text{since } k^{3} \equiv 1 \pmod{n}$$

and therefore $\alpha\beta$ is of order 3. One may note that

$$\alpha^{-1}\beta\alpha = \beta^{k},$$

because

$$\alpha^{-1}\beta\alpha = \{a,b\} \xrightarrow{\alpha^{-1}} \{a,b^{k^2}\} \xrightarrow{\beta} \{ab^{k-1},b^{k^2}\} \xrightarrow{\alpha} \{ab^{k(k-1)},b^{k^3}\}$$

$$= \{a,b\} \longrightarrow \{ab^{k(k-1)},b\}, \quad k^3 \equiv 1 \pmod{n},$$

but

$$\beta^{k} = \{a,b\} \longrightarrow \{ab^{k(k-1)},b\},$$

therefore

$$\alpha^{-1}\beta\alpha = \beta^{k}.$$

Now, when $3|n$, then $H_1 = \{\alpha,\beta\}$ whose defining relations are

$$\alpha^3 = \beta^{\frac{n}{3}} = (\alpha\beta)^3 = e, \quad \alpha^{-1}\beta\alpha = \beta^{k}$$

and this H_1 is $I(G_n)$. When $3 \nmid n$ then $H_2 = \{\alpha,\beta\}$ whose defining relations are:

$$\alpha^3 = \beta^n = (\alpha\beta)^3 = e, \quad \alpha^{-1}\beta\alpha = \beta^{k},$$

and this H_2 is $I(G_n)$. Therefore $I(G_n)$ is always generated by α and β.

Again, consider the following automorphisms:

$$\alpha = \{a,b\} \longrightarrow \{a,b^{k}\}$$

which was shown to be inner and of order 3,

$$\beta_1 = \{a,b\} \longrightarrow \{ab,b\}$$

and this is obviously of order n, whether $3|n$ or $3 \nmid n$,

$$\alpha\beta_1 = \{a,b\} \to \{ab,b^k\}$$
$$(\alpha\beta_1)^2 = \{a,b\} \to \{ab^{k+1},b^{k^2}\}$$
$$(\alpha\beta_1)^3 = \{a,b\} \to \{ab^{k^2+k+1},b^{k^3}\}$$
$$= \{a,b\} \to \{a,b\} ,$$

therefore $\alpha\beta_1$ is of order 3. Again one may note that

$$\alpha^{-1}\beta_1\alpha = \beta_1^k ,$$

because

$$\alpha^{-1}\beta_1\alpha = \{a,b\} \xrightarrow{\alpha^{-1}} \{a,b^{k^2}\} \xrightarrow{\beta_1} \{ab,b^{k^2}\} \xrightarrow{\alpha} \{ab^k,k^3\}$$
$$= \{a,b\} \to \{ab^k,b\} , \quad k^3 \equiv 1 \pmod{n}$$

but

$$\beta_1^k = \{a,b\} \to \{ab^k,b\}$$

i.e.

$$\alpha^{-1}\beta_1\alpha = \beta_1^k .$$

Therefore, $H_3 = \{\alpha,\beta_1\}$ is an analogue of order $3n$ and $H_3 \sim G_n$. When $3 \nmid n$ then β_1 is generated by β and hence β_1 will be inner and therefore $H_3 = H_2$. When $3|n$ then β_1 is not inner, for the simple reason that $H_3 \neq H_1$, since H_1 is $I(G_n)$ and is of order n, while H_3 is of order $3n$.

More generally one may consider the automorphism

$$\beta_p = \{a,b\} \to \{ab^p,b\} , \quad \text{where } (p,n) = 1 ,$$

then

$$(\beta_p)^m = \{a,b\} \to \{ab^{mp},b\},$$

and since

$$mp \not\equiv 0 \pmod{n}, \qquad (p,n) = 1 \quad \text{for all} \quad 0 < m < n$$

and

$$mp \equiv 0 \pmod{n}, \qquad (p,n) = 1 \quad \text{when} \quad m = n \quad \text{or} \quad m = nt,$$

therefore β_p is of order n,

$$(\alpha\beta_p) = \{a,b\} \rightarrow \{ab^p, b^k\}$$

$$(\alpha\beta_p)^2 = \{a,b\} \rightarrow \{ab^{p(k+1)}, b^{k^2}\}$$

$$(\alpha\beta_p)^3 = \{a,b\} \rightarrow \{ab^{p(k^2+k+1)}, b^{k^3}\}$$

$$= \{a,b\} \quad \{a,b\}.$$

therefore $\alpha\beta_p$ is of order 3. Again, it can be proved easily that $\alpha^{-1}\beta_p\beta = \beta_p^k$. Hence, $H_p = \{\alpha, \beta_p\}$ is also an analogue group of order $3n$. In fact $H_p = H_3$, since β generates β_p.

Still more generally when one considers the automorphism

$$\beta_j = \{a,b\} \rightarrow \{ab^j, b\}, \qquad (j,n) = d_j,$$

then

$$(\beta_j)^m = \{a,b\} \rightarrow \{ab^{mj}, b\}$$

$$= \{a,b\} \rightarrow \{a, \ b\}, \qquad \text{when} \quad mj \equiv 0 \pmod{n}.$$

Let $j = d_j z$, and $n = d_j x$, then $mj = m\, d_j z$ and hence $mz \equiv 0 \pmod{x}$, but $(z,x) = 1$, therefore $m = x$ or $m = yx$, but here the least integer

that will do is $m = x = \frac{n}{d_j}$, therefore β_j is of order $m = \frac{n}{d_j}$. Here also one can show easily that $\alpha\beta_j$ is of order 3 and $\alpha^{-1}\beta_j\alpha = \beta_j^k$. Hence, $H_j = \{\alpha,\beta_j\}$ is an analogue group of order $\frac{3n}{d_j}$.

BIBLIOGRAPHY

Entries are arranged chronologically)

Group Theory

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

2. Carmichael, R.D., Introduction to the Theory of Group of Finite Order. Dover ed. New York, Dover Publications, Inc., 1956.

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

Number Theory

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