Spring 4-30-1943

A Study of Certain Substitution Groups

Merle Mitchell

MITCH-
ELL

SUBSTI-
TUTION
GROUPS

NAME AND ADDRESS	DATE

A STUDY OF CERTAIN SUBSTITUTION GROUPS

by

Merle Mitchell

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Arts in Mathematics

University of New Mexico
1943

This thesis, directed and approved by the candidate's committee, has been accepted by the Graduate Committee of the University of New Mexico in partial fulfillment of the requirements for the degree of

MASTER OF ARTS

G. P. Hammond
DEAN

April 30, 1943
DATE

Thesis committee

C. B. Barber
CHAIRMAN

C. V. Newsom

C. L. Gibson

TABLE OF CONTENTS

CHAPTER		PAGE
I.	INTRODUCTION	1
	1. The Problem	1
	2. Organization	2
II.	THE GROUP IN GENERAL	4
	1. Definition of a Group	4
	2. Examples of Groups	5
	3. Definition of a Subgroup	8
III.	SUBSTITUTION GROUPS	9
	1. Definition of a Substitution Group	9
	2. Explanation of Permutation Symbols	9
	3. Explanation of Multiplication of Permutation Symbols	10
	4. A Multiplication Table	11
	5. Degree and Order	12
	6. Rotations of a Square into Itself Considered as a Cyclic Substitution Group	12
	7. Cyclic Groups and Generators	14
IV.	SYMMETRIES	16
	1. Symmetries of a Space	16
	2. The Octic Group and Its Subgroups	16
	3. The Group of the Cube With One Vertex Held Fixed	18

CHAPTER		PAGE
V.	THE GROUP OF THE CUBE	20
	1. The Twenty-eight Geometrical Symmetries of the Cube	20
	2. A Multiplication Table of These Elements.	21
	3. Introduction of Twenty New Permutations on the Vertices of the Cube	21
	4. Total of Elements in the Group of the Cube	22
VI.	SUBGROUPS	27
	1. Order of Subgroups; Theorem 1	27
	2. The Group of the Cube as a Subgroup . .	29
	3. Application of the Theorem to Some Subgroups of the Group of the Cube . .	29
VII.	TRANSFORMS	34
	1. Definition of Transforms	34
	2. Method of Obtaining Transforms; Theorem 2	34
	3. Invariant Substitutions	35
	4. Conjugate Groups	37
	5. Invariant Subgroups	37
VIII.	POSITIVE AND NEGATIVE SUBSTITUTIONS. . . .	40
	1. Factoring Permutations into Transpositions	40
	2. Factored Form of a Permutation; Theorem 3	40

CHAPTER PAGE

3. Relation of Positive and Negative Elements to the Nature of the Group; Theorem 4 40

4. Application to the Group of the Cube . . 43

IX. CONCLUSION 44

BIBLIOGRAPHY 47

CHAPTER I

INTRODUCTION

1. The Problem. This thesis purposes to study a certain group of movements which can be expressed as substitutions. The group of movements which send a square into itself is to be studied as a group of eight substitutions on the vertices for the purpose of leading up to the real problem of this paper. From the octic group, it is natural to proceed to a study of the movements which send a cube into itself. In particular, it is the aim of this thesis to discover the group of the cube and to analyze some of its properties. There are twenty-eight rotations and reflections with respect to diagonals and central axes of the cube which possess special geometrical properties. One of the problems of this thesis is to determine whether or not these twenty-eight elements constitute a group. Once the group of the cube has been determined, other problems are those of finding subgroups within the original group and of enumerating their properties. This paper is to be concerned chiefly with subgroups composed entirely of elements from the twenty-eight rotations and reflections with the special geometrical properties. Also a few theorems relative to groups in general will be demonstrated and application will be made to the group of the cube.

1. The problem. [illegible]
certain group of [illegible]
stitutions. The group of [illegible]
1930 itself is to be [illegible]
tions on the vertices [illegible]
cal problem of this paper [illegible]
natural to proceed [illegible]
ance into itself. [illegible]
Maschke to discover the group of [illegible]
of the pre-orbital [illegible]
[illegible] with respect [illegible]
cube sub-groups [illegible]
the problems of [illegible]
these twenty-eight [illegible]
group of the cube [illegible]
those of finding sub-groups [illegible]
enumerating their properties. [illegible]
chiefly with sub-groups [illegible]
the twenty-eight [illegible]
geometrical properties. [illegible]
groups in general [illegible]
be made to the group of the cube.

Thus the problems of this thesis may be summarized as follows:

(1) The determination of the group of the cube.

(2) The discovery of subgroups within the original group, especially subgroups composed entirely of elements with particular geometrical properties.

(3) An enumeration of the properties of such subgroups.

(4) The demonstrations of theorems relative to groups in general and their application to the group of the cube.

2. Organization. The work is organized into seven chapters, the first two of which are composed largely of definitions and explanations of symbols. In these chapters are found the definition of a group, examples of groups, the concept of the substitution group, an explanation of the permutation symbols and their multiplication, and the idea of cyclic groups. The third chapter treats the symmetries of the square, the octic group, and the group of the cube with one vertex held fixed. The ideas of this chapter are extended in the fourth chapter to the isometries of the three dimensional space, and, in particular, to the group of the cube. A multiplication table of the twenty-eight movements with special geometrical properties is given to discover whether or not

Thus [illegible] as follows:

(1) The definition [illegible]

(2) The [illegible] of [illegible] ecological [illegible] and [illegible] other [illegible]

(3) [illegible] and [illegible].

(4) The [illegible] to [illegible] the role.

B. [illegible]. [illegible] computers, the [illegible] definitions and [illegible] are found the [illegible] concept of the [illegible] mutation symbols [illegible] cyclic groups. The [illegible] squares, [illegible] vertex [illegible] the [illegible] graphs, and, [illegible] identification [illegible] generational [illegible]

these elements form a group. By this table, the group of the cube is determined. The fifth chapter begins with a theorem about the order of subgroups and then demonstrates how several subgroups of the group of the cube satisfy the conditions of the theorem. A study of transforms and their relation to invariant substitutions and subgroups is contained in the sixth chapter. The paper concludes with some considerations in regard to positive and negative substitutions and their relation to the nature of the group of the cube.

CHAPTER II

THE GROUP IN GENERAL

1. Definition of a Group. Let e_i represent a set of elements for which there is defined a binary operation $\circ$. Then the elements e_i form a group when combined according to this law of operation if the following conditions, or axioms, are satisfied:

(1) The result obtained by $e_i \circ e_j$ is another element e_k of the set, where i, j, k are not necessarily distinct. (This condition is commonly referred to as the "group property.")

(2) There is an identity element I in the set such that

$$e_i \circ I = e_i = I \circ e_i.$$

(3) Every element e_i has an inverse e_i^{-1} in the set such that

$$e_i \circ e_i^{-1} = I = e_i^{-1} \circ e_i.$$

(4) The associative law holds for the defined law of combination; that is,

$$e_i \circ (e_j \circ e_k) = (e_i \circ e_j) \circ e_k.$$

The operation $\circ$ may be any law of combination, but in the theory of groups it is generally called multiplication, and the result obtained by the given operation is called the product. If multiplication is commutative for every element

[illegible]

1. Definition of a Group. Let G represent a set of elements for which there is defined a binary operation [illegible]. Then the elements $a, b, c, \ldots$ form a group with respect to this law of operation if the following conditions, or axioms, are satisfied:

(1) The result [illegible] of any two elements [illegible] ment a_i of the set [illegible] tions. (This [illegible] "group property.")

(2) There [illegible] that

$$[illegible]$$

(3) Every element [illegible] such that

$$[illegible]$$

(4) The associative [illegible] of combinations [illegible]

$$[illegible]$$

The operation [illegible] the theory of groups it is [illegible] and the result obtained [illegible] product. If multiplication is [illegible]

[illegible]

in the group, the group is said to be an Abelian* group.

2. Examples of Groups. The positive rational numbers form a group when the operation $\circ$ is particularized to be ordinary multiplication. The product of any two positive rational numbers is another positive rational number, so axiom (1) is satisfied. The identity element in this group is 1 since multiplication by 1 leaves every element unchanged, thus fulfilling axiom (2). The inverse of each element is its reciprocal which is in the group; thus condition (3) is satisfied. Of course, the associative law required by axiom (4) holds under multiplication. Since the operation is also commutative, the group is Abelian.

On the other hand, the positive rational numbers do not form a group under division; for, although the group property holds, although the identity 1 is contained in the set, and although the inverse of each element, which in this case is the element itself, is present, yet the associative law does not hold in general as can be seen from the following:

$$\frac{a}{b} \div \left(\frac{c}{d} \div \frac{e}{f}\right) = \frac{\frac{a}{b}}{\frac{c}{d} \cdot \frac{f}{e}} = \frac{a}{b} \cdot \frac{de}{cf} = \frac{ade}{bcf}$$

*So called from Niels Henrik Abel (1802-1829), a Norwegian mathematician, who made valuable contributions to the theory of groups by his study of commutative groups.

$$\left(\frac{a}{b} \div \frac{c}{d}\right) \div \frac{e}{f} = \frac{\frac{a}{b} \cdot \frac{d}{c}}{\frac{e}{f}} = \frac{ad}{bc} \cdot \frac{f}{e} = \frac{adf}{bce}$$

But $\frac{ade}{bcf} \neq \frac{adf}{bce}$ if e and f are distinct, i.e., if $\left|\frac{e}{f}\right| \neq 1$.

The four elements 1, -1, i, and -i form a group under ordinary multiplication. The multiplication table* appears below:

	1	-1	-i	i
1	1	-1	-i	i
-1	-1	1	i	-i
i	i	-i	1	-1
-i	-i	i	-1	1

---

*In this and in subsequent multiplication tables, the elements in the first vertical column may be regarded as operating on those in first horizontal row. The products of an element in the first row by the elements in the first column appear in the column beneath the multiplicand. Thus a product of two elements is found in the place where the row determined by the multiplier and the column determined by the multiplicand intersect.

The identity element is 1 and each element has an inverse as is evident from the table. The associative law holds for this type of multiplication.

The integers 1, 5, 7, and 11 form a group under multiplication with respect to the modulus 12. The identity element is 1; the associative law holds for ordinary multiplication; the presence of inverses for each element is evident from the table which shows no new elements added by the process of combination. This group is Abelian.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

The positive and negative integers and zero form a group under addition. The sum of any two such integers is another integer. The identity element in such a group is zero since any element combined with zero by addition leaves that element unchanged. The inverse of each integer is the corresponding integer of opposite sign; while zero is its own inverse. It is obvious that the associative law holds for addition.

[illegible]

[illegible]

[illegible]				

[illegible]

3. Definition of a Subgroup. If among the elements of a group, it is possible to select certain elements which also satisfy the conditions for a group, then these elements are said to constitute a subgroup of the original group. The identity element must be included in such a subgroup. It is interesting to note that the identity I alone forms a subgroup of every group.

The even positive and negative integers and zero form a group under addition. The sum of two even integers is obviously an even integer; the identity element is zero; the inverse of an element is the element of the same numerical value with opposite sign; the associative law holds. This group is a subgroup of the group of all integers mentioned above.

CHAPTER III

SUBSTITUTION GROUPS

1. Definition of a Substitution Group. If the existence of a set of letters is assumed, a group results when all the possible interchanges of the letters are considered. Such a group is called a substitution group. For example, beginning with the three letters a, b, and c, a substitution group is obtained by considering the six possible interchanges of these letters. These substitutions are as follows: (abc), (acb), (ab), (bc), (ac), and I.

2. Explanation of Permutation Symbols. The symbol (abc) means that a is replaced by b, b by c, and c by a; the symbol (acb) means that a is replaced by c, c by b, and b by a; (ab) implies that a and b are interchanged while c remains unchanged; (bc) means that b is replaced by c and c by b while a is replaced by itself; similarly (ac) indicates a replacement of a by c and c by a while b is unchanged; the identity I means that each letter is replaced by itself. A substitution such as (abc) or (ac) is called a cycle because the symbol indicates the replacement of each letter by the one which follows it and the replacement of the last letter by the first. Thus, it is clear that (abc) = (cab) = (bca), and that (ac) = (ca). A cycle on two letters such as (bc) is said to be a transposition.

1. Definitions [illegible] of [illegible]

substitution of a set of [illegible] when all the possible [illegible] con- sidered. Such a group is called [illegible]. For example, beginning with the three letters [illegible] mutations [illegible] able interchanges [illegible] are as follows: [illegible]

2. [illegible]

(abc) [illegible] symbol (abc) [illegible] a; (ab) implies [illegible] unchanged [illegible] a is [illegible] of a by [illegible] I [illegible] tion [illegible] symbol [illegible] which [illegible] given. Thus, [illegible] (ab) = (ca). [illegible] is a [illegible].

3. **Explanation of Multiplication of Permutation Symbols.** In order to show that the six substitutions constitute a group, it is necessary to define a law of combination. If (abc) is multiplied by (acb), the product is obtained by the following procedure. In the first cycle a is replaced by b; in the second cycle b is replaced by a; hence a is ultimately replaced by itself. Again, in the first cycle, b becomes c; in the second cycle c becomes b; hence b is replaced by itself. In the first cycle c becomes a which in the second cycle becomes c; hence c is replaced by itself. According to the definition of the identity then, the product

$$(abc)\circ(bac) = I.$$

To multiply (ab) by (bc), it is observed that in the first cycle a is replaced by b and in the second b by c so that a becomes c; again, in the first substitution c is replaced by itself, and in the second c is replaced by b so that c becomes b; in the first cycle b becomes a and in the second a is replaced by itself so that b is replaced by the original letter with which the product cycle was begun. Thus the product cycle is complete and the result is

$$(ab)\circ(bc) = (acb).$$

It is to be noted that the multiplication in this group is not commutative since

$$(ab)\circ(bc) = (acb)$$

while

$$(bc)\circ(ab) = (abc).$$

4. <u>A Multiplication Table</u>. Let a multiplication table now be constructed to show that no new substitutions are introduced when any two of the six are multiplied according to the law of combination.

	I	(abc)	(acb)	(ab)	(bc)	(ac)
I	I	(abc)	(acb)	(ab)	(bc)	(ac)
(acb)	(acb)	I	(abc)	(ac)	(ab)	(bc)
(abc)	(abc)	(acb)	I	(bc)	(ac)	(ab)
(ab)	(ab)	(ac)	(bc)	I	(acb)	(abc)
(bc)	(bc)	(ab)	(ac)	(abc)	I	(acb)
(ac)	(ac)	(bc)	(ab)	(acb)	(abc)	I

It is evident from the table that all products of one substitution by another yield no new substitutions. Also it can be seen from the table that I is the identity element and that every element has an inverse in the original six substitutions. Clearly the associative law would hold in this case. There are five subgroups present; namely,

I	I, bc
I, ab	I, abc, acb
I, ac	

5. Degree and Order. The degree of a substitution group is defined to be the number of distinct letters found in its substitutions. The order of the group is the number of distinct substitutions or elements in the group. The order of a substitution is defined as the number of letters included in the cycle under consideration. A group consisting of all the possible $\lfloor n$ substitutions on n letters constitute a symmetric group. Thus the group discussed in the preceding paragraph is the symmetric group of degree three and order six.

6. Rotations of a Square Into Itself Considered as a Cyclic Substitution Group. Let us now consider a square with vertices, a, b, c, and d, and let the law of operation be a set of clockwise rotations around the center 0 of the square through angles of $\frac{k\pi}{2}$ radians where $k = 0, 1, 2, \cdots$.

It is evident from the table that [illegible] property of [illegible] stitution [illegible] [illegible]. [illegible] can be seen from the table [illegible] the identity element and that every element has an inverse in the set of substitutions. Clearly the [illegible] in this case. There are five [illegible]

I [illegible]

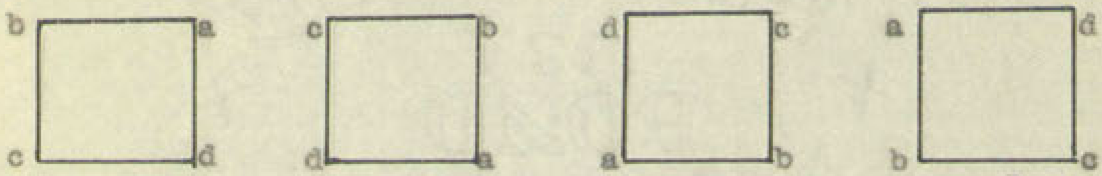
I, a [illegible]

I, ac [illegible]

b. Integral and [illegible]. [illegible] group is defined as the [illegible] in its substitutions [illegible] of standard [illegible] order of a group [illegible] included in the [illegible] ing of all the [illegible] stitute a [illegible] preceding [illegible] and order etc.

c. [illegible] a [illegible] with [illegible] [illegible] square [illegible]

It is clear that the combination of any two such rotations would be equivalent to a single rotation. A rotation through π radians combined with one through $\frac{\pi}{2}$ radians would be equivalent to a single rotation through $\frac{3\pi}{2}$ radians. The following figures illustrate the movements of the square for 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ radians.



I R R' R"

The original position of the square is given in the first figure and is denoted by I. A rotation about the center through the angle of $\frac{\pi}{2}$ is given in the second figure and is denoted by R. A rotation through π is shown in the third figure and is denoted by R'. A rotation through $\frac{3\pi}{2}$ is given in the fourth figure and is denoted by R". Evidently any rotation through an angle of $K\frac{\pi}{2}$ radians where $K \geq 4$ is equivalent to one of the rotations through $k\frac{\pi}{2}$ radians where $k = 0, 1, 2, 3$. Thus only I, R, R', and R" need be considered as elements of the set. Following the notation scheme indicated above,

$$R = (abcd) \qquad R' = (ac)(bd)$$

$$R'' = (adcb)$$

Thus when the square is rotated through $\frac{\pi}{2}$ radians, the vertices are changed or permuted so that a goes into b, b into c, c into d, and d into a; that is, a cyclic substitution on the four letters is obtained. When the square is rotated through π radians, the vertices a and c are interchanged independently of the interchange between b and d.

If the sixteen products arising from the four symbolic representations of the rotations were to be computed, no new substitutions on the four vertices would be discovered; this is obvious from the nature of the law of combination. Thus the group property is satisfied. The identity element in this set is the rotation through 0 radians which has been represented by I. Every element has an inverse in the set, for I is its own inverse; R and R" are inverses; and R' is its own inverse. Obviously the associative law holds. It has thus been proved that this set of rotations forms a group. In fact, it may be said that the set of rotations constitutes a substitution group of degree four and order four.

7. <u>Cyclic Groups and Generators</u>. A group is said to be <u>cyclic</u> if all of its elements are powers of one certain element which is called the <u>generator</u> of the group. The group I, R, R', and R" is a cyclic group in which R or R" may be selected as generators. It might be pointed out that R' does not generate the group since $R' \circ R' = I$, and $I \circ R' = R'$, and thus the various powers of R' do not yield either R or R".

thus when the [illegible]

coincides [illegible]

taken [illegible]

also on the [illegible]

rotated through [illegible]

changed into [illegible]

If A [illegible]

substitutions [illegible]

substitutions [illegible]

is obvious [illegible]

the group [illegible]

this [illegible]

reported [illegible]

I is the [illegible]

can however [illegible]

this [illegible]

fact, it [illegible]

substitution [illegible]

V. [illegible]

be cyclic [illegible]

element [illegible]

T, R, R', [illegible]

selected [illegible]

not generate the [illegible]

and thus the [illegible]

By a consideration of the geometrical meaning of these symbols, it is also clear why R and R" both generate the group while R' does not. Symbolically the powers of the generator R are the following:

$R = (abcd)$

$R^2 = (abcd)\circ(abcd) = (ac)(bd) = R'$

$R^3 = (ac)(bd)\circ(abcd) = (adcb) = R''$

$R^4 = (adcb)\circ(abcd) = (ac)(bd)\circ(ac)(bd) = I$

Obviously R^5 would be equivalent to R, R^6 to R^2, etc.; that is, in general, R^n would be equivalent to R^i where $i = 0, 1, 2, 3$ if $n \equiv i \pmod 4$.

A substitution group is said to be generated by a set of substitutions if every substitution of the group can be obtained by combining those of the set. For example, the symmetric group of order six is generated by any two of its distinct substitutions of order two. This may be illustrated by the use of the substitutions (ab) and (bc):

$(ab)\circ(bc) = (acb)$	$(bc)\circ(acb) = (ac)$
$(ab)\circ(ab) = I$	$(acb)\circ(acb) = (abc)$
$(ab)\circ(acb) = (bc)$	$(bc)\circ(abc) = (ab)$

The six substitutions obtained by these multiplications are indeed the elements of the symmetric group of order six and thus (ab) and (bc) are a set of substitutions which generate the group.

CHAPTER IV

SYMMETRIES

1. Symmetries of a Space. One of the most interesting phases of group theory is concerned with the various movements which transform a space into itself. Many times the elements of such a group are symmetries of the space with respect to certain axes, diagonals, or points.

2. The Octic Group and Its Subgroups. The group of rotations through $k\frac{\pi}{2}$ radians which transform the square into itself is in reality a subgroup of the group of symmetries of the square. This group represents transformations of the space of the plane and are called isometries of the plane. Let the original position of the square be assumed to be that of the illustration in the preceding chapter. If the four movements I, R, R', and R" have the same meaning as there, it is necessary only to define the remaining elements and to prove the existence of a group. Let M_x represent a reflection in the horizontal axis through O; M_y a reflection in the vertical axis through O; D_1 a reflection in the diagonal connecting the vertices a and c; D_2 a reflection in the diagonal connecting b and d. Just as the rotations were represented symbolically as substitutions, so may substitutions be constructed to represent the reflections. Thus the elements

are:

I	$M_x = (ad)(bc)$
$R = (abcd)$	$M_y = (ab)(cd)$
$R' = (ac)(bd)$	$D_1 = (bd)$
$R'' = (adcb)$	$D_2 = (ac)$

To prove that these eight elements constitute a group, let us construct a multiplication table from which it can be observed that no new elements are introduced into the set by multiplication, and that each element has an inverse in the set. Then since there is an identity element, and since the associative law always holds for rotations and reflections of this type, this is found to be a group. It is interesting to note that this group is not commutative. The multiplication table follows on page 19. The subgroups of this octic group, as the group of the square is called, are nine in number including the identity element. They are:

I, (ac)(bd), (abcd), (adcb)

I, (ac)(bd), (ac), (bd)

I, (ac)(bd), (ab)(cd), (ad)(bc)

I, (ac)(bd)

I, (ac)

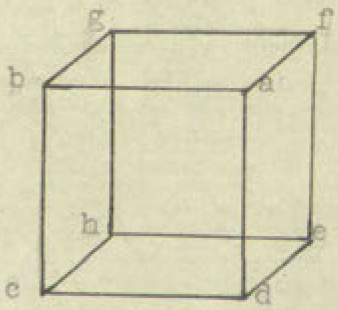
I, (bd)

I, (ab)(cd)

I, (ad)(bc)

I

3. <u>The Group of the Cube With One Vertex Held Fixed</u>. The isometries of a three dimensional space transform a cube into itself. Let a cube be considered with the vertices a, b, c, d, e, f, g, and h as in the figure, and let it be assumed that vertex a is held fixed. In finding the symmetries of the cube under this condition, it is noted that the vertices b, d, f (adjacent to a) can then be permuted in 3 ways. When one vertex and the three adjacent vertices are in a known position, all vertices of the cube are in a fixed position. Thus there are six symmetries of the cube with one vertex held fixed.



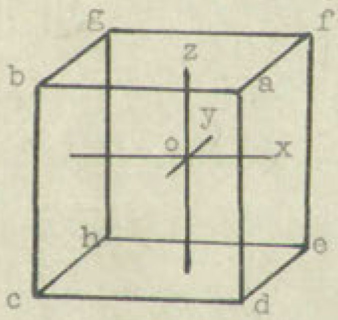
In the particular case in which a is held fixed, the symmetries are (bfd), (bdf), (bd), (df), (bf), and I. These six substitutions have the same form as the substitutions of the symmetric group of order six. In fact, a one-to-one correspondence between the two may be set up. Thus, it is unnecessary to construct a multiplication table to determine whether or not these elements form a group since the table would clearly have the same form as that for the symmetric group of order six. In this way, the existence of a group on the vertices b, d, f is established.

	I	(abcd)	(ac)(bd)	(adcb)	(ad)(bc)	(ab)(cd)	(bd)	(ac)
I	I	(abcd)	(ac)(bd)	(adcb)	(ad)(bc)	(ab)(cd)	(bd)	(ac)
(abcd)	(abcd)	(ac)(bd)	(adcb)	I	(ac)	(bd)	(ad)(bc)	(ab)(cd)
(ac)(bd)	(ac)(bd)	(adcb)	I	(abcd)	(ab)(cd)	(ad)(bc)	(ac)	(bd)
(adcb)	(adcb)	I	(abcd)	(ac)(bd)	(bd)	(ac)	(ab)(cd)	(ad)(bc)
(ad)(bc)	(ad)(bc)	(bd)	(ab)(cd)	(ac)	I	(ac)(bd)	(abcd)	(adcb)
(ab)(cd)	(ab)(cd)	(ac)	(ad)(bc)	(bd)	(ac)(bd)	I	(adcb)	(abcd)
(bd)	(bd)	(ab)(cd)	(ac)	(ad)(bc)	(adcb)	(abcd)	I	(ac)(bd)
(ac)	(ac)	(ad)(bc)	(bd)	(ab)(cd)	(abcd)	(adcb)	(ac)(bd)	I

CHAPTER V

THE GROUP OF THE CUBE

1. The Twenty-eight Geometrical Symmetries of the Cube. Let us now proceed to the study of the various transformations on the vertices of a cube. Let the vertices of the cube be a, b, c, d, e, f, g, and h, and let the original position of the cube be that shown in the figure.



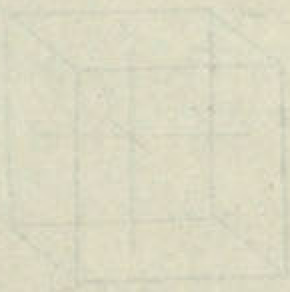
Let one horizontal axis through the center 0 of the cube be the x-axis; let the vertical axis through 0 be the z-axis; and let the axis through 0 perpendicular to the xz plane be the y-axis. Then the various rotations and reflections which transform the cube into itself can be represented as permutations on the vertices.

There follows on page 24 a chart of the 28 symmetries such as are described above; to each symmetry there has been assigned a special symbol; moreover, the permutation on the vertices occasioned by each symmetry is listed.

It was demonstrated in the last chapter that the

[illegible]

1. The [illegible] of the Cube. Let us [illegible] [illegible] [illegible] trans- formations on the vertices of a cube [illegible] [illegible] [illegible] [illegible]



[illegible]

[illegible]

[illegible]

symmetries of a square constitute a group and hence it might be assumed that the twenty-eight reflections and rotations which transform the cube into itself also form a group. It is easy, however, to show that these twenty-eight symmetries do not satisfy the group property, for there are many pairs of elements whose product is outside the set of twenty-eight elements. For instance, if R_z is multiplied by R'_x, or R_x by P_1, a substitution not included in the given elements is obtained.

2. <u>A Multiplication Table of These Elements.</u> Let us nevertheless construct the multiplication table of these twenty-eight elements. From the table, it can be determined how many new elements are introduced in the process of combining the given substitutions, and also it can be discovered what subgroups, if any, exist among the twenty-eight substitutions. Such a multiplication table is worked out on the folding chart at the end of this thesis.

3. <u>Introduction of Twenty New Permutations on the Vertices of the Cube.</u> Among the 28 x 28 products there is a total of twenty new elements which recur again and again. Symbols for these twenty elements and the corresponding substitution on the eight vertices are given in the next chart.

[illegible] be assumed [illegible] which [illegible] In many, however, [illegible] do not satisfy the [illegible] of elements above [illegible] elements. For instance, [illegible] T_c by [illegible] is obtained.

4. [illegible] twenty-eight elements, [illegible] how many [illegible] at that [illegible] alloyed. [illegible] rolling [illegible]

5. Influence of [illegible] lattice [illegible] level of [illegible] symbols [illegible]

Symbol	Permutation	Symbol	Permutation
1. E'_{ah}	(ah)(bgfedc)	11. II_3	(af)(be)(ch)(dg)
2. E''_{ah}	(ah)(bcdefg)	12. II_4	(ah)(bg)(cf)(de)
3. E'_{be}	(be)(afghcd)	13. II_5	(ad)(be)(cf)(gh)
4. E''_{be}	(be)(adchgf)	14. II_6	(ah)(bc)(dg)(ef)
5. E'_{cf}	(cf)(adehgb)	15. IV_1	(aceg)(bdhf)
6. E''_{cf}	(cf)(abghed)	16. IV_2	(acge)(bhfd)
7. E'_{dg}	(dg)(abchef)	17. IV_3	(agec)(bfhd)
8. E''_{dg}	(dg)(afehcb)	18. IV_4	(agce)(bhdf)
9. II_1	(ah)(be)(cd)(fg)	19. IV_5	(aecg)(bfdh)
10. II_2	(ab)(cf)(dg)(eh)	20. IV_6	(aegc)(bdfh)

4. <u>Total of Elements in the Group of the Cube.</u> It is interesting to observe that, while the twenty-eight possible rotations and reflections do not themselves constitute a group, yet under multiplication they generate besides themselves twenty more elements, and also to observe that the forty-eight permutations so obtained do constitute the group of the cube. The twenty additional substitutions are also called symmetries of the cube, but they do not have special geometrical properties as do the original twenty-eight. If we should extend the multiplication table to contain the products of the first twenty-eight elements by the additional

twenty and the 20 x 20 products of the new permutations by themselves, we would discover no new elements, for it is a well known fact that these forty-eight symmetries form a group.*

---

* Birkhoff and Mac Lane, A Survey of Modern Algebra, p. 128.

SYMBOL		PERMUTATION ON VERTICES	EXPLANATION
1.	I	I	Original position of cube
2.	R_x	(adef)(bchg)	Rotation through $\frac{\pi}{2}$ radians about x axis
3.	R'_x	(ae)(bh)(cg)(df)	Rotation through π radians about x axis
4.	R''_x	(afed)(bghc)	Rotation through $3\frac{\pi}{2}$ radians about x axis
5.	R_z	(abgf)(ched)	Rotation through $\frac{\pi}{2}$ radians about z axis
6.	R'_z	(ag)(bf)(ce)(dh)	Rotation through π radians about z axis
7.	R''_z	(afgb)(cdeh)	Rotation through $3\frac{\pi}{2}$ radians about z axis
8.	R_y	(adcb)(ehgf)	Rotation through $\frac{\pi}{2}$ radians about y axis
9.	R'_y	(ac)(bd)(eg)(fh)	Rotation through π radians about y axis
10.	R''_y	(abcd)(efgh)	Rotation through $3\frac{\pi}{2}$ radians about y axis
11.	M_{xy}	(ad)(bc)(ef)(gh)	Reflections in the xy plane
12.	M_{xz}	(af)(bg)(ch)(de)	Reflection in the xz plane
13.	M_{yz}	(ab)(cd)(eh)(fg)	Reflection in the yz plane
14.	M_o	(ah)(be)(cf)(dg)	Reflection in the origin

SYMBOL	PERMUTATION ON VERTICES	EXPLANATION
15. D_{ah}	(bdf)(ceg)	Rotation about diagonal ah through π radians in the counterclockwise direction
16. D_{be}	(acg)(dhf)	Rotation about diagonal be through π radians in the counterclockwise direction
17. D_{gd}	(aec)(bfh)	Rotation about diagonal gd through π radians in the counterclockwise direction
18. D_{fc}	(age)(bhd)	Rotation about diagonal fc through π radians in the counterclockwise direction
19. D'_{ah}	(bfd)(cge)	Rotation about diagonal ah through π radians in the clockwise direction
20. D'_{be}	(agc)(dfh)	Rotation about diagonal be through π radians in the clockwise direction
21. D'_{gd}	(ace)(bhf)	Rotation about diagonal gd through π radians in the clockwise direction
22. D'_{fc}	(aeg)(bdh)	Rotation about diagonal fc through π radians in the clockwise direction
23. P_1	(bd)(eg)	Reflection in the diagonal plane afhc
24. P_2	(cg)(df)	Reflection in the diagonal plane abhe

SYMBOL	PERMUTATION ON VERTICES	EXPLANATION
25. P_3	(ac)(fh)	Reflection in the diagonal plane bged
26. P_4	(ae)(bh)	Reflection in the diagonal plane cdfg
27. P_5	(bf)(ce)	Reflection in the diagonal plane adhg
28. P_6	(ag)(dh)	Reflection in the diagonal plane bcef

CHAPTER VI

SUBGROUPS

Some theorems concerning the various properties of groups in general will now be proved and the results will be applied to the group of the cube.

1. Order of Subgroups. Theorem 1. The order of every subgroup is a divisor of the order of the original group.

To prove this fundamental theorem, let G be a finite group* of order N, and let g be a subgroup of G of order n. Let the elements of g be

$$x_1, x_2, \cdots, x_n.$$

Since n N, some element a of G not included in g can be found. If all the elements of g are multiplied by a, there is obtained the set of elements

$$ax_1, ax_2, \cdots, ax_n.$$

Obviously these elements are all contained in G since a and x_i where $i = 1, 2, \cdots, n$ are members of G. These elements are distinct from each other inasmuch as

$$ax_i = ax_j, \text{ where } i \neq j$$

implies that $x_i = x_j$, a situation which cannot exist in a subgroup. Also these elements are distinct from the elements of

---

* A finite group is a group having a finite number of elements.

the subgroup, for

$$ax_i = x_j$$

implies that $a = x_j \circ x_i^{-1}$, or that a is in the subgroup g contrary to the selection of a. If this set together with the subgroup does not exhaust the array of N elements of G, then there is some element b of G not included in either. Then by multiplying each element of g by b, another set of elements results as follows:

$$bx_1, bx_2, \cdots, bx_n.$$

All of these elements are distinct from each other and from the elements of the subgroup by the same sort of reasoning as above and are also distinct from the elements ax_i for

$$bx_j = ax_i$$

implies that $b = ax_i \circ x_j^{-1}$ or that b is in the set of elements ax_i contrary to the selection of b. It is clear that, since G is a finite group, the elements of G will be exhausted after a finite number of such operations. Hence the elements of G can be written in rectangular array as follows:

$$\begin{array}{llll} x_1, & x_2, & \cdots, & x_n \\ ax_1, & ax_2, & \cdots, & ax_n \\ bx_1, & bx_2, & \cdots, & bx_n \\ \vdots & \vdots & & \vdots \\ zx_1, & zx_2, & \cdots, & zx_n \end{array}$$

where the first row represents the subgroup g of the group G and where the subsequent rows are the products of the elements

the subgroup [illegible]

[illegible]

implies that [illegible]
[illegible]
the subgroup [illegible]
Then [illegible]
Then [illegible]
elements [illegible]

All of these [illegible]
the [illegible]
as [illegible]

implies that [illegible]
[illegible]
since [illegible]
after [illegible]
of a [illegible]

[illegible]

where the [illegible]
and where the [illegible]

of g by distinct elements of G. Thus evidently the order n of the subgroup must be a divisor of the order N of the group.

2. <u>The Group of the Cube as a Subgroup</u>. The group of order forty-eight under consideration is in reality a subgroup of the symmetric group of order $\underline{|8}$ which results from all the possible substitutions on the eight letters involved. Clearly the order forty-eight is a divisor of the order $\underline{|8}$. Within the subgroup it is possible to select numerous subgroups. According to the theorem just proved, the orders of these subgroups must be factors of the order forty-eight.

3. <u>Application of the Theorem to Some Subgroups of the Group of the Cube</u>. Of special interest are those subgroups which are composed entirely of elements from the twenty-eight symmetries with particular geometrical properties which generated the group of order forty-eight. Perhaps the first subgroups that come to mind are the three cyclic, Abelian subgroups of order four composed of the identity element and the rotations about the three axes. These subgroups are

$$I,\ R_x,\ R'_x,\ R''_x$$
$$I,\ R_z,\ R'_z,\ R''_z$$
$$I,\ R_y,\ R'_y,\ R''_y$$

of g by distinct diagonals [illegible]
a of the subgroup [illegible]
group.

2. [illegible]
of order forty-eight [illegible]
subgroup of the [illegible]
from all the [illegible]
volved. [illegible]
order 12. [illegible]
[illegible]
the [illegible]
[illegible]

3. [illegible]
the group of [illegible]
groups and [illegible]
eight [illegible]
[illegible] and the group [illegible]
subgroups that [illegible]
[illegible]
the rotations [illegible]

These groups are generated by either R_i or R''_i, where $i = x, y, z$, as explained previously. Each of these groups contains a subgroup of order two as follows:

$$I, R'_x; \; I, R'_z; \text{ and } I, R'_y .$$

Another subgroup of order four is composed of the identity element and the rotations about the x, y, and z axes through π radians; the elements are

$$I, R'_x, R'_y, R'_z.$$

This subgroup is Abelian though not cyclic as can be seen by an inspection of the multiplication table.

Among the rotations about the several diagonals of the cube, there are four subgroups of order three. These cyclic groups are as follows:

$$I, D_{ah}, D'_{ah}$$

$$I, D_{be}, D'_{be}$$

$$I, D_{gd}, D'_{gd}$$

$$I, D_{fc}, D'_{fc}$$

The Abelian group of order eight composed of the elements

$$I, M_{xy}, M_{xz}, M_{yz}, M_o, R'_x, R'_y, R'_z$$

contains some very interesting subgroups. Besides the subgroups on the identity and rotations about the axes indicated above, there are four other subgroups of order two. They are composed of the identity and the reflections in

in the three central planes and in the origin. These subgroups are

$$I,\ M_{xy};\ I,\ M_{xz};\ I,\ M_{yz};\ \text{and}\ I,\ M_o.$$

An unusual property of this group of order eight is that each element combined with the identity forms a subgroup of order two. The group also contains four subgroups of order four as follows:

$$I,\ R'_x,\ R'_y,\ R'_z$$

$$I,\ M_{yz},\ M_o,\ R'_x$$

$$I,\ M_{xy},\ M_o,\ R'_z$$

$$I,\ M_{xz},\ M_o,\ R'_y$$

The first of these subgroups has already received comment. The last three are rather surprising combinations of elements to form a group. That these elements do form groups, however, can be verified easily from the multiplication table.

There is a subgroup of order twelve composed of the identity element, the rotations about the axes through π radians, and the rotations about the four diagonals of the cube. It is as follows:

$$I,\ R'_x,\ R'_z,\ R'_y,\ D_{ah},\ D_{be},\ D_{gd},\ D_{fc},$$
$$D'_{ah},\ D'_{be},\ D'_{gd},\ D'_{fc}.$$

Its subgroups have already been mentioned.

A consideration of the elements which transform the

cube into itself by reflections in the diagonal planes leads to a number of unexpected combinations of elements to form subgroups. There are the following three subgroups of order eight:

$$I,\ R_x,\ R'_x,\ R''_x,\ M_{xz},\ M_{xy},\ P_2,\ P_4$$

$$I,\ R_y,\ R'_y,\ R''_y,\ M_{yz},\ M_{xy},\ P_1,\ P_3$$

$$I,\ R_z,\ R'_z,\ R''_z,\ M_{yz},\ M_{xz},\ P_5,\ P_6$$

Besides those subgroups already mentioned in connection with other groups, the three subgroups above contain the following three subgroups respectively:

$$I,\ R'_x,\ P_2,\ P_4$$

$$I,\ R'_y,\ P_1,\ P_3$$

$$I,\ R'_z,\ P_5,\ P_6$$

It might be pointed out that the six reflections in the diagonal planes never form a subgroup when combined among themselves with the identity element, but they must be taken two or three at a time in combination with other selected sets of elements. Below are four subgroups of order six composed of these reflections taken three at a time in combination with the identity element and the rotations about the diagonals:

$$I,\ D_{ah},\ D'_{ah},\ P_1,\ P_2,\ P_5$$

$$I,\ D_{be},\ D'_{be},\ P_2,\ P_3,\ P_6$$

$I, D_{gd}, D'_{gd}, P_3, P_4, P_5$

$I, D_{fc}, D'_{fc}, P_1, P_4, P_6$

CHAPTER VII

TRANSFORMS

1. Definition of Transforms. If S and Q are any substitutions, then the substitution T is called the transform of S as regards Q if T satisfies the relation

$$Q^{-1} \cdot S \cdot Q = T$$

where Q^{-1} is the inverse of Q. Thus if two substitutions S and Q of a group are given, it is possible to find a third substitution T by the relation above. A simple method for determining T will now be given.

2. Method of Obtaining Transforms. Theorem 2. The transform T of S as regards Q may be determined by replacing each letter of S by the one which replaces it in Q.

For the proof, let Q be a cyclic substitution such that

$$Q = (x_1x'_1x_2x'_2 \cdots x_nx'_n)$$

in which x_i where $i = 1, 2, \cdots, n$ represents any letter of the substitution and x'_i represents the letter into which x_i is carried. Then

$$Q^{-1} = (x'_nx_n \cdots x'_2x_2x'_1x_1).$$

Suppose $S = x_1x_2 \cdots x_n$. It is to be observed that these notations are very general and include all cases since in any particular case x_i might be identically equal to x'_i, or x_i

[illegible]

[illegible]

1. [illegible]

[illegible]

2. [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

might not appear in the representation at all. According to the definition of T, then

$$Q^{-1} \circ S \circ Q = T, \text{ or}$$

$$(x'_n x_n \cdots x'_2 x_2 x'_1 x_1) \circ (x_1 x_2 \cdots x_n) \circ (x_1 x'_1 x_2 x'_2 \cdots x_n x'_n) =$$

$$(x_1)(x_2)\cdots(x_n)(x'_1 x'_2 \cdots x'_n) = (x'_1 x'_2 \cdots x'_n) = T.$$

Hence to obtain T, simply replace each letter of S by the one which replaces it in Q. Thus it is clear that S and T will always be of the same degree.

For example, to find the transform of R_x as regards R'_x, each letter of R_x is replaced by the one which replaces it in R'_x. Since $R_x = (adef)(bchg)$ and $R'_x = (ae)(bh)(cg)(df)$, then $T = (efad)(hgbc)$ which is the result obtained by multiplying out $(R'_x)^{-1} \circ R_x \circ R'_x$. By substituting R'_x for $(R'_x)^{-1}$ the product is as follows:

$$R'_x \circ R_x \circ R'_x = (ae)(bh)(cg)(df) \circ (adef)(bchg) \circ (ae)(bh)(cg)(df) =$$
$$(adef)(hgbc) = T.$$

3. <u>Invariant</u> <u>Substitutions</u>. If a substitution is transformed into itself by every substitution of a group, then that substitution is said to be <u>invariant</u> under the group. For example, M_o is invariant under the groups I, R_i, R'_i, and R''_i where $i = x, y, z$, as can be verified from the following table in which T, S, and Q have the same meanings as in the preceding paragraph and for which

$$S = M_o = (ah)(be)(cf)(dg).$$

S	Q_1	T_1	Q_2	T_2	Q_3	T_3
M_o	I	M_o	I	M_o	I	M_o
M_o	$R_x=(adef)(bchg)$	M_o	$R_z=(abgf)(ched)$	M_o	$R_y=(adcb)(ehgf)$	M_o
M_o	$R'_x=(ae)(bh)(cg)(df)$	M_o	$R'_z=(ag)(bf)(dh)(ce)$	M_o	$R'_y=(ac)(bd)(eg)(fh)$	M_o
M_o	$R''_x=(afed)(bghc)$	M_o	$R''_z=(afgb)(cdeh)$	M_o	$R''_y=(abcd)(efgh)$	M_o

If a substitution remains invariant under the group of which it is a member, then it is called an <u>invariant substitution</u> of the group. M_o is accordingly an invariant substitution of the group

$$I,\ M_{xy},\ M_{xz},\ M_{yz},\ R'_x,\ R'_y,\ R'_z,\ M_o$$

as can be seen from the following table in which again

$$S = M_o = (ah)(be)(cf)(dg).$$

S	Q	T
M_o	I	M_o
M_o	M_{xy} = (ad)(bc)(ef)(gh)	M_o
M_o	M_{xz} = (af)(bg)(ch)(de)	M_o
M_o	M_{yz} = (ab)(cd)(eh)(fg)	M_o
M_o	R'_x = (ae)(bh)(cg)(df)	M_o
M_o	R'_y = (ac)(bd)(eg)(fh)	M_o
M_o	R'_z = (ag)(bf)(ce)(dh)	M_o
M_o	M_o = (ah)(be)(cf)(dg)	M_o

4. Conjugate Groups. If each substitution of a group G is transformed by a substitution Q, another group G' of the same order results. G' is called the transform or conjugate of G with respect to Q. For example, if every substitution of the group I, R_x, R'_x, and R''_x is transformed by D_{ah}, the group I, R_z, R'_z, and R''_z is obtained, and if the same group is transformed by D'_{ah}, the group I, R_y, R'_y, and R''_y is obtained. Similarly if I, R_x, R'_x, and R''_x are transformed by D_{be}, D_{gd}, or D_{fc}, the group I, R_z, R'_z, and R''_z results; whereas if the same group is transformed by D'_{be}, D'_{gd}, or D'_{fc}, the Group I, R_y, R'_y, and R''_y results.

5. Invariant Subgroups. When it happens that the conjugate G' is the same group as G, then the group G is said to

invariant under the substitution Q. Thus the group I, R_x, R'_x, and R''_x is invariant under each of the substitutions M_{xy}, M_{xz}, and M_{yz} as can be easily demonstrated.

If a substitution is transformed into itself by some of the elements of a group but not by the rest, then those elements which leave the substitution invariant form a subgroup of the original group. An illustration of this fact is furnished by the transforms of R''_x by the group:

$$I, M_{xy}, M_{xz}, M_{yz}, R'_x, R'_y, R'_z, M_o.$$

The following table shows that I, M_{yz}, M_o, and R'_x leave R''_x invariant while M_{xy}, M_{xz}, R'_y, and R'_z transform R''_x into a new substitution. Thus I, M_{yz}, M_o, and R'_x form a subgroup of the original group as can be easily verified. For the table below

$$S = R''_x = (afed)(bghc).$$

S	Q	T
R''_x	I	R''_x
R''_x	M_{xy} = (ad)(bc)(ef)(gh)	R_x
R''_x	M_{xz} = (af)(bg)(ch)(de)	R_x
R''_x	M_{yz} = (ab)(cd)(eh)(fg)	R''_x
R''_x	M_o = (ah)(be)(cf)(dg)	R''_x
R''_x	R'_x = (ae)(bh)(cg)(df)	R''_x
R''_x	R'_y = (ac)(bd)(eg)(fh)	R_x
R''_x	R''_z = (ag)(bf)(ce)(dh)	R_x

Similarly if R''_y and R''_z are transformed by the elements of this group, two more subgroups are determined. The substitutions which leave R''_y invariant are I, M_{xz}, M_o, and R'_y; those leaving R''_z invariant are I, M_{xy}, M_o, and R'_z.

CHAPTER VIII

POSITIVE AND NEGATIVE SUBSTITUTIONS

1. Factoring Permutations Into Transpositions. Any permutation can be expressed as the product of transpositions. In order to show the truth of this statement, it is necessary to consider only a cyclic permutation since from the nature of a permutation, it is clear that any permutation may be written as the product of cycles no two of which have a letter in common. Thus a permutation containing more than one cycle would involve but a reapplication of the principle applied to a single cycle. That any permutation can be factored into the product of transpositions follows immediately from the identity below in which P represents any cyclic permutation.

$$P \equiv (x_1x_2x_3\cdots x_n) \equiv (x_1x_2)(x_1x_3)\cdots(x_1x_n).$$

As a matter of fact, P might have been factored into transpositions in a great number of ways. For example,

$$P \equiv (x_1x_2x_3\cdots x_n) \equiv (x_2x_1)(x_2x_3)\cdots(x_2x_n) \quad \text{or}$$

$$P \equiv (x_1x_2x_3\cdots x_n) \equiv (x_1x_2)(x_2x_3)\cdots(x_{n-1}x_n).$$

A permutation is said to be positive if it factors into an even number of transpositions, and negative if into an odd number.

2. Factored Form of a Permutation. Theorem 3. The number of transpositions into which a permutation can be

factored is always odd or always even.

Consider the product

$$
\begin{aligned}
(x_1-x_2)\cdot(x_1-x_3)\cdot(x_1-x_4)\cdot\cdots\cdot(x_1-x_n)& \\
\cdot(x_2-x_3)\cdot(x_2-x_4)\cdot\cdots\cdot(x_2-x_n)& \\
\cdot(x_2-x_4)\cdot\cdots\cdot(x_3-x_n)& \\
\cdots\cdots\cdots& \\
\cdot(x_{n-1}-x_n)& = X.
\end{aligned}
$$

If the transposition (x_1x_2) is performed on this product, then

$$
\begin{aligned}
(x_2-x_1)\cdot(x_2-x_3)\cdot(x_2-x_4)\cdot\cdots\cdot(x_2-x_n)& \\
\cdot(x_1-x_3)\cdot(x_1-x_4)\cdot\cdots\cdot(x_1-x_n)& \\
\cdot(x_3-x_4)\cdot\cdots\cdot(x_3-x_n)& \\
\cdots\cdots\cdots& \\
\cdot(x_{n-1}-x_n)& = -X.
\end{aligned}
$$

Thus the transposition (x_1x_2) changes the sign of the product. Similarly every transposition (x_ix_j) where $i \neq j$ and where $i, j = 1, 2, 3, \cdots, n$ changes the sign of the product. Hence an even number of transpositions leaves X unaltered, whereas an odd number changes the sign of X. Now since the various sets of transpositions into which a permutation is factored must affect the product X in the same way as the permutation, then the number of transpositions for any given permutation must be always odd or always even.

A corollary of this theorem is that the product of permutations is positive or negative according as the total number of negative permutations in the product is even or odd. The identity element is regarded as positive. The inverse of a permutation is positive or negative according as the permutation itself is positive or negative.

3. Relation of Positive and Negative Elements to the Nature of the Group. Theorem 4. The positive elements of a permutation group either constitute the entire group or form a subgroup of half the order of the original group.

The positive elements of a group always form a group since the identity is a positive element and the inverses of positive elements are positive. If not all the elements of a group are positive, suppose the positive, distinct elements are $I, x_1, x_2, \cdots, x_n$ and the negative, distinct elements are $y_1, y_2, \cdots, y_m$.

Then,

$$y_1 \cdot x_1, y_1 \cdot x_2, \cdots, y_1 \cdot x_n$$

are all negative by the corollary above and are distinct since $y_1 \cdot x_i = y_1 \cdot x_j$ where $i \neq j$ would imply $x_i = x_j$ contrary to the assumption of distinctness. Hence there are at least as many negative elements as positive in the group. The products

$$y_1 \cdot y_1, y_1 \cdot y_2, \cdots, y_1 y_m$$

are all positive and distinct. Hence there are at least as many positive as negative elements in the group. Thus the positive elements of a group either compose the entire group or constitute a subgroup of half the order of the original group.

4. Application to the Group of the Cube. In the group of the cube, some of the substitutions are already factored into transpositions; namely,

$$R'_x,\ R'_z,\ R'_y,\ M_{xy},\ M_{xz},\ M_{yz},\ M_o,$$

$$P_1,\ P_2,\ P_3,\ P_4,\ P_5,\ P_6.$$

All of these are positive permutations. Then the permutations

$$R_x,\ R''_x,\ R_z,\ R''_z,\ R_y,\ R''_y$$

are all positive since each is composed of the product of two negative permutations. The rotations about the diagonals of the cube are composed of the product of two positive permutations, and hence these substitutions are also positive. Thus twenty-eight out of the forty-eight elements are positive, and by use of the theorem that the positive elements either comprise the entire group or constitute a group of half the order of the original group, it is possible to state that the remainder of the elements are likewise positive. Obviously the group of the cube is composed entirely of positive elements.

[illegible]

group. [illegible]

4. [illegible] [illegible]

group [illegible]

fashioned into [illegible]

All [illegible]

[illegible]

CHAPTER IX

CONCLUSION

The problems set forth at the beginning of this thesis have thus been studied in some detail as indicated below:

(1) The group of the cube is composed of forty-eight elements expressed as permutations on the vertices, twenty-eight of which possess special geometrical properties.

(2) A number of subgroups of this group composed entirely of the elements with geometrical meaning have been exhibited.

(3) Properties of order and invariance have been discussed with respect to these subgroups.

(4) The following theorems have been proved and applied to the group of the cube:

Theorem 1. The order of every subgroup is a divisor of the order of the original group.

Theorem 2. The transform T of S as regards Q may be determined by replacing each letter of S by the one which replaces it in Q.

Theorem 3. The number of transpositions into which a permutation can be factored is always odd or always even.

Theorem 4. The positive elements of a permutation group either constitute the entire group or form a subgroup of half the order of the original group.

	R_x	R'_x	R''_x	R_z	R'_z	R''_z	R_y	R'_y	R''_y	M_{xy}	M_{xz}	M_{yz}	D_{ah}	D_{be}	D_{gd}	D_{fc}	D'_{ah}	D'_{be}	D'_{gd}	D'_{fc}	M_o	P_1	P_2	P_3	P_4	P_5	P_6
R_x	R'_x	R''_x	I	D'_{gd}	II_1	D_{fc}	D_{be}	II_2	D_{ah}	P_2	P_4	IV_1	II_3	II_4	R_y	R''_y	R_z	R''_z	II_5	II_6	IV_3	E'_{dg}	M_{xz}	E'_{cf}	M_{xy}	E''_{be}	E''_{ah}
R'_x	R''_x	I	R_x	II_5	R'_y	II_6	II_4	R'_z	II_3	M_{xz}	M_{xy}	M_o	D_{fc}	D_{gd}	D_{be}	D_{ah}	D'_{gd}	D'_{fc}	D'_{ah}	D'_{be}	M_{yz}	IV_4	P_4	IV_5	P_2	IV_2	IV_6
R''_x	I	R_x	R'_x	D'_{ah}	II_2	D'_{be}	D_{gd}	II_1	D_{fc}	P_4	P_2	IV_3	R''_y	R_y	II_4	II_3	II_5	II_6	R_z	R''_z	IV_1	E'_{be}	M_{xy}	E'_{ah}	M_{xz}	E''_{cf}	E''_{dg}
R_z	D_{be}	II_6	D'_{fc}	R'_z	R''_z	I	D'_{ah}	II_5	D'_{gd}	IV_2	P_6	P_5	R_x	II_2	R''_x	II_1	II_3	R''_y	II_4	R_y	IV_6	E''_{be}	E'_{dg}	E''_{cf}	E'_{ah}	M_{xz}	M_{yz}
R'_z	II_2	R'_y	II_1	R''_z	I	R_z	II_3	R'_x	II_4	M_o	M_{yz}	M_{xz}	D_{be}	D_{ah}	D_{fc}	D_{gd}	D'_{fc}	D'_{gd}	D'_{be}	D'_{ah}	M_{xy}	IV_5	IV_1	IV_4	IV_3	P_6	P_5
R''_z	D_{ah}	II_5	D_{gd}	I	R_z	R'_z	D'_{fc}	II_6	D'_{be}	IV_6	P_5	P_6	II_2	R_x	II_1	R''_x	R_z	II_4	R''_y	II_3	IV_2	E''_{dg}	E'_{cf}	E''_{ah}	E'_{be}	M_{yz}	M_{xz}
R_y	D_{fc}	II_3	D'_{ah}	D_{be}	II_4	D_{gd}	R'_y	R''_y	I	P_1	IV_5	P_3	R''_z	II_6	II_5	R_z	II_2	R''_x	R_x	II_1	IV_4	M_{yz}	E''_{dg}	M_{xy}	E''_{be}	E'_{cf}	E'_{ah}
R'_y	II_1	R'_z	II_2	II_6	R'_x	II_5	R''_y	I	R_y	M_{yz}	M_o	M_{xy}	D_{gd}	D_{fc}	D_{ah}	D_{be}	D'_{be}	D'_{ah}	D'_{fc}	D'_{gd}	M_{xz}	P_3	IV_3	P_1	IV_1	IV_6	IV_2
R''_y	D'_{gd}	II_4	D'_{be}	D_{fc}	II_3	D_{ah}	I	R_y	R'_y	P_3	IV_4	P_1	II_5	R_z	R''_z	II_6	R''_x	II_2	II_1	R_x	IV_5	M_{xy}	E''_{cf}	M_{yz}	E''_{ah}	E'_{be}	E'_{dg}
M_{xy}	P_4	M_{xz}	P_2	IV_2	M_o	IV_6	P_3	M_{yz}	P_1	I	R'_x	R'_y	E'_{be}	E'_{ah}	E'_{cf}	E'_{dg}	E''_{cf}	E''_{dg}	E''_{be}	E''_{ah}	R'_z	R''_y	R''_x	R_y	R_x	II_5	II_6
M_{xz}	P_2	M_{xy}	P_4	P_5	M_{yz}	P_6	IV_5	M_o	IV_4	R'_x	I	R'_z	E'_{dg}	E'_{cf}	E'_{ah}	E'_{be}	E''_{be}	E''_{ah}	E''_{cf}	E''_{dg}	R'_y	II_3	R_x	II_4	R''_x	R_z	R''_z
M_{yz}	IV_1	M_o	IV_3	P_6	M_{xz}	P_5	P_1	M_{xy}	P_3	R'_y	R'_z	I	E'_{cf}	E'_{dg}	E'_{be}	E'_{ah}	E''_{dg}	E''_{cf}	E''_{ah}	E''_{be}	R'_x	R_y	II_2	R''_y	II_1	R''_z	R_z
D_{ah}	II_5	D_{gd}	R''_z	R''_y	D_{fc}	II_3	R_x	D_{be}	II_2	E'_{cf}	E'_{be}	E'_{dg}	D'_{ah}	D'_{gd}	D'_{fc}	D'_{be}	I	R'_z	R'_y	R'_x	E'_{ah}	P_2	P_5	IV_1	IV_6	P_1	IV_4
D_{be}	II_6	D_{fc}	R_z	II_4	D_{gd}	R_y	II_2	D_{ah}	R_x	E'_{dg}	E'_{ah}	E'_{cf}	D'_{fc}	D'_{be}	D'_{ah}	D'_{gd}	R'_z	I	R'_x	R'_y	E'_{be}	IV_2	P_6	P_2	IV_2	IV_5	P_3
D_{gd}	R''_z	D_{ah}	II_5	R_y	D_{be}	II_4	II_1	D_{fc}	R''_x	E'_{be}	E'_{cf}	E'_{ah}	D'_{be}	D'_{fc}	D'_{gd}	D'_{ah}	R'_y	R'_x	I	R'_z	E'_{dg}	IV_3	IV_6	P_4	P_5	P_3	IV_5
D_{fc}	R_z	D_{be}	II_6	II_3	D_{ah}	R''_y	R''_x	D_{gd}	II_1	E'_{ah}	E'_{dg}	E'_{be}	D'_{gd}	D'_{ah}	D'_{be}	D'_{fc}	R'_x	R'_y	R'_z	I	E'_{cf}	P_4	IV_2	IV_3	P_6	IV_4	P_1
D'_{ah}	R_y	D'_{fc}	II_3	II_2	D'_{be}	R''_x	II_5	D'_{gd}	R_z	E''_{be}	E''_{dg}	E''_{cf}	I	R'_y	R'_x	R'_z	D_{ah}	D_{fc}	D_{be}	D_{gd}	E''_{ah}	P_5	P_1	IV_2	IV_5	P_2	IV_3
D'_{be}	R''_y	D'_{gd}	II_4	R''_x	D'_{ah}	II_2	R''_z	D'_{fc}	II_6	E''_{ah}	E''_{cf}	E''_{dg}	R'_y	I	R'_z	R'_x	D_{gd}	D_{be}	D_{fc}	D_{ah}	E''_{be}	IV_6	P_3	P_6	IV_4	IV_3	P_2
D'_{gd}	II_4	D'_{be}	R''_y	II_1	D'_{fc}	R_x	R_z	D'_{ah}	II_5	E''_{cf}	E''_{ah}	E''_{be}	R'_x	R'_z	I	R'_y	D_{fc}	D_{ah}	D_{gd}	D_{be}	E''_{dg}	IV_2	IV_4	P_5	P_3	P_4	IV_1
D'_{fc}	II_3	D'_{ah}	R_y	R_x	D'_{gd}	II_1	II_6	D'_{be}	R''_z	E''_{dg}	E''_{be}	E''_{ah}	R'_z	R'_x	R'_y	I	D_{be}	D_{gd}	D_{ah}	D_{fc}	E''_{cf}	P_6	IV_5	IV_6	P_1	IV_1	P_5
M_o	IV_3	M_{yz}	IV_1	IV_6	M_{xy}	IV_2	IV_4	M_{xz}	IV_5	R'_z	R'_y	R'_x	E'_{ah}	E'_{be}	E'_{dg}	E'_{cf}	E''_{ah}	E''_{be}	E''_{dg}	E''_{cf}	I	II_4	II_1	II_3	II_2	II_6	II_5
P_1	E''_{be}	IV_5	E''_{dg}	E'_{dg}	IV_4	E'_{be}	M_{xy}	P_3	M_{yz}	R_y	II_3	R''_y	P_5	IV_2	IV_6	P_6	P_2	IV_3	IV_1	P_4	II_4	I	D'_{ah}	R'_y	D'_{fc}	D_{ah}	D_{fc}
P_2	M_{xy}	P_4	M_{xz}	E''_{cf}	IV_3	E''_{dg}	E'_{cf}	IV_1	E'_{dg}	R_x	R''_x	II_2	P_1	P_3	IV_5	IV_4	P_5	P_6	IV_2	IV_6	II_1	D_{ah}	I	D_{be}	R'_x	D'_{ah}	D'_{be}
P_3	E''_{ah}	IV_4	E''_{cf}	E'_{ah}	IV_5	E'_{cf}	M_{yz}	P_1	M_{xy}	R''_y	II_4	R_y	IV_6	P_6	P_5	IV_2	IV_3	P_2	P_4	IV_1	II_3	R'_y	D'_{be}	I	D'_{gd}	D_{gd}	D_{be}
P_4	M_{xz}	P_2	M_{xy}	E''_{be}	IV_1	E''_{ah}	E'_{ah}	IV_3	E'_{be}	R''_x	R_x	II_1	IV_4	IV_5	P_3	P_1	IV_2	IV_6	P_5	P_6	II_2	D_{fc}	R'_x	D_{gd}	I	D'_{gd}	D'_{fc}
P_5	E'_{cf}	IV_6	E'_{be}	M_{yz}	P_6	M_{xz}	E''_{be}	IV_2	E''_{cf}	II_5	R''_z	R_z	P_2	IV_1	P_4	IV_3	P_1	IV_4	P_3	IV_5	II_6	D'_{ah}	D_{ah}	D'_{gd}	D_{gd}	I	R'_z
P_6	E'_{dg}	IV_2	E'_{ah}	M_{xz}	P_5	M_{yz}	E''_{dg}	IV_6	E''_{ah}	II_6	R_z	R''_z	IV_1	P_2	IV_2	P_4	IV_5	P_3	IV_4	P_1	II_5	D'_{fc}	D_{be}	D'_{be}	D_{fc}	R'_z	I

BIBLIOGRAPHY

Birkhoff, Garrett and Mac Lane, Saunders, A Survey of Modern Algebra, Macmillan Company, New York, 1941.

Carmichael, Robert D., Introduction to the Theory of Groups of Finite Order, Ginn and Company, Dallas, 1937.

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

Lieber, Lillian R., Galois and the Theory of Groups: A Bright Star in Mathesis, The Science Press Printing Company, Lancaster, Pennsylvania, 1932.

Mathewson, Louis Clark, Elementary Theory of Finite Groups, Houghton Mifflin Company, Dallas, 1930.

Miller, G. A., Blichfeldt, H. F., and Dickson, L. E., Theory and Applications of Finite Groups, John Wiley and Sons, Incorporated, New York, 1916.

IMPORTANT!

Special care should be taken to prevent loss or damage of this volume. If lost or damaged, it must be paid for at the current rate of typing.