1968

Groups

Janie Ferguson
Ouachita Baptist University

GROUPS

A Paper

Presented to

the Mathematics Department of

Ouachita Baptist University

In Fulfillment

of the Requirements for

Honors Special Studies H291

Mathematics

by

Janie Ferguson

January 1968

GROUPS

1. Abstract Groups

In the study of modern algebra it is convenient to introduce the abstract concept of a group, G, with one binary operation indicated as multiplication. By definition, a group G is a system of elements which is closed under a single-valued binary operation which is associative, contains an element satisfying the identity law, and with each element another element (called its inverse) satisfying the inverse law. In product notation, with "e" for the identity, the three laws defining groups are

ASSOCIATIVE LAW: $a(bc) = (ab)c$ for all a, b, c;

IDENTITY LAW: $ae = ea = a$ for all a;

INVERSE LAW: $aa^{-1} = a^{-1}a = e$ for each a and some a^{-1}.

The positive real numbers form a group under multiplication. Associative: $a(bc) = (ab)c$; Identity: $a \times 1 = 1 \times a = a$, where $e = 1$; Inverse: $a \times 1/a = 1/a \times a = 1$. However, they do not form a group under addition. (The starred laws are the ones which are not satisfied.) Associative: $(a + b) + c = a + (b + c)$; *Identity: $a + 0 = 0 + a = a$, but 0 is not a positive real number; *Inverse: $a + (-a) = (-a) + a = 0$, but the inverse is always a negative number.

In the field Z_{11} of integers modulo 11, the set of numbers (1, 3, 4, 5, 9) is a group under multiplication.

x	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

The associative law holds, the identity is 1, and the inverses are: $1^{-1} = 1$, $3^{-1} = 4$, $4^{-1} = 3$, $5^{-1} = 9$, $9^{-1} = 5$.

The set of irrational numbers under multiplication is not a group. It is not closed: $\sqrt[n]{a_1} \times \sqrt[n]{a_2} \times \ldots \times \sqrt[n]{a_n} = a$ and the identity element is 1, but is not contained in the set.

The following Cayley square describes a group. For every element the associative property holds, the identity element is c, and the inverses are: $a^{-1} = d$, $c^{-1} = c$, $b^{-1} = b$, $d^{-1} = a$.

	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

All integers under the operation of subtraction do not form a group. *Associative: $a-(b - c) \neq (a - b) - c$; Identity: $a - 0 = a$; Inverse: $a - a = 0$.

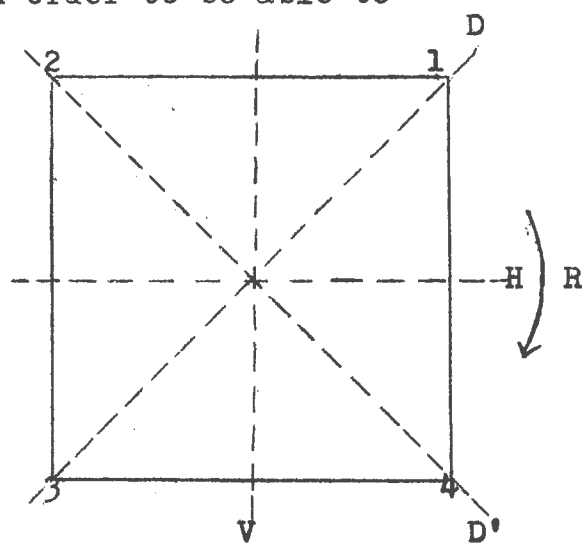
2. Symmetries

The algebra of symmetries has its genesis in the fact that two motions can be "multiplied" by performing them in succession. A symmetry of a geometrical figure is a one-one transformation of its points which preserves distance. In the case of the symmetries of the square, any symmetry must carry the vertex 1 into one of the four possible vertices and for each such choice there are exactly two symmetries. Thus all together there are eight symmetries.

R: a 90° rotation clockwise around the origin

R', R'': similar rotations through 180° and 270°

These three are rotational symmetry. The square also has refexive symmetry; it can be carried into itself by the following rigid reflections: H: a reflection in the horizontal axis through the origin; V: a reflection in the vertical axis through the origin; D: a reflection in the diagonal in quadrants I and III; D': a reflection in the diagonal in quadrants II and IV. The so-called identity motion I is considered a (degenerate) symmetry, in order to be able to multiply all pairs of symmetries.



It can be shown that this set of symmetries comprises a group, known as the group of the symmetries of the square. This group is non-abelian. By use of the Cayley square the complete multiplication table of the group may be shown.

	I	R	R'	R''	H	V	D	D'
I	I	R	R'	R''	H	V	D	D'
R	R	R'	R''	I	D	D'	V	H
R'	R'	R''	I	R	V	H	D'	D
R''	R''	I	R	R'	D'	D	H	V
H	H	D'	V	D	I	R'	R''	R
V	V	D	H	D'	R'	I	R	R''
D	D	H	D'	V	R	R''	I	R
D'	D'	V	D	H	R''	R	R'	I

Most of the group properties can be read directly from the table. The existence of an identity states that some row and the corresponding column must be replicas of the top heading and of the left heading respectively. The group is commutative if and only if its table is symmetric about the principle diagonal (which extends from upper left to lower right).

In the same manner, the symmetries of an equilateral triangle may be computed.

R: a 120° rotation clockwise around center 0.

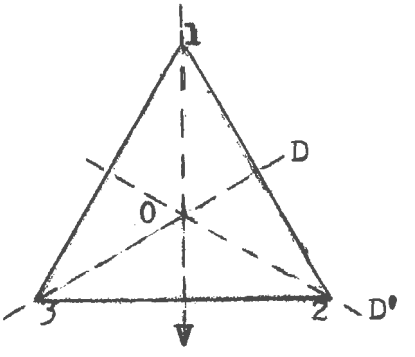
R': a similar rotation through 240°.

V: a reflection in the vertical axis through 0.

D: a reflection in the diagonal going through 3.

D': a reflection in the diagonal going through 2.

	I	R	R'	V	D	D'
I	I	R	R'	V	D	D'
R	R	R'	I	D'	V	D
R'	R'	I	R	D	D'	V
V	V	D	D'	I	R	R'
D	D	D'	V	R'	I	R
D'	D'	V	D	R	R'	I



3. Groups of Transformations

The algebra of symmetry can be extended to one-one transformations of any set S of elements. It is often suggestive to think of the set S as a "space" and of its

elements as "points", but the rules of calculation are the same no matter what S is. By the transformation ϕ: S$\rightarrow$ T from a (nonempty) set S into a set T is meant a rule ϕ which assigns to each element p E S a unique image element pϕ in T. The set S is called the domain of ϕ , and T its codomain. The product or composite $\phi\psi$ of two transformations is defined as the result of performing them in succession; first ϕ, then ψ, provided the codomain of ϕ is the domain of ψ.

By a "group of transformation" on a "space" S is meant any set G of one-one transformations ϕ of S onto S such that

(1) the identity transformation of S is in G;

(2) if ϕ is in G, so is its inverse ϕ^{-1};

(3) if ϕ and ψ are in G, so is their product $\phi\psi$.

If S consists of all real numbers and the transformations to be considered have the form $x\phi = ax + b$, in the following cases some of the sets of all possible ϕ's with coefficients a and b are groups of transformations, while others are not.

(a). If a and b are rational numbers, a group of transformations is formed.

$x\phi = ax + b$ and $x\psi = a_1x + b_1$

$x\phi^{-1} = \frac{x - b}{a}$ (Inverse)

$(x\phi^{-1})\phi = a(\frac{x - b}{a}) + b = x - b + b = x$

$\therefore \phi^{-1}\phi = I.$ (Identity)

$(x\phi)\psi = a_1(ax + b) + b_1 = a_1ax + a_1b + b_1$ (Closure)

$\therefore \phi\psi$ is in the set defined.

Since all three stipulations of a group of transformations are met, it is a group.

(b). If a = 1, b is an odd integer, a group of transformations is not formed.

$x\phi = x + (2n + 1)$

$x\phi^{-1} = x - (2n + 1)$ (Inverse)

$(x\phi^{-1})\phi = x - (2n + 1) + 2n + 1 = x + 0.$

$\therefore \phi^{-1}\phi = I.$ (Identity)

However, b in this case is 0, which is not an odd integer.

(c). If $a \neq 0$, a is an integer, b is a real number, then a group of transformations is formed.

$x\phi = a_1 x + \sqrt{b_1}$

$x\phi^{-1} = \frac{x - \sqrt{b_1}}{a_1}$ (Inverse)

$(x\phi^{-1})\phi = a_1\left(\frac{x - \sqrt{b_1}}{a_1}\right) + \sqrt{b_1} = x - \sqrt{b_1} + \sqrt{b_1} = x.$

$\therefore \phi^{-1}\phi = I$ (Identity)

If $x\phi = a_2 x + \sqrt{b_2}$, then $x\phi\phi = a_1(a_2 x + \sqrt{b_2}) + \sqrt{b_1}$

$= a_1 a_2 x + a_1\sqrt{b_2} + \sqrt{b_1}$ (Closure).

4. Isomorphism

The concept of isomorphism is valuable because it gives form to the recognition that the same abstract group situation can arise in entirely different contexts. By an isomorphism between two groups G and G' is meant a one-one correspondence $a \leftrightarrow a'$ between their elements which preserves group multiplication -- i.e., which is such that if $a \leftrightarrow a'$ and $b \leftrightarrow b'$, then $ab \leftrightarrow a'b'$. a' is called the image of a. The fact that isomorphic groups are abstractly the same can be seen in a number of examples.

Let G = multiplicative group on the fourth roots of

unity, and let G' = additive group of the residue classes modulo four whose elements are 0, 1, 2, 3.

G		G'
1	⟷	0
i	⟷	1
-1	⟷	2
-i	⟷	3

G		G'
1	⟷	0
i	⟷	3
-1	⟷	2
-i	⟷	1

The group tables reveal the isomorphisms of these groups.

X	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	3	2	1
0	0	3	2	1
3	3	2	1	0
2	2	1	0	3
1	1	0	3	2

From these tables, the theorem that the identity elements correspond and the inverses of corresponding elements correspond can be seen.

The group of rotations of a square and the multiplicative group of 1, 5, 8, 12 mod 13 are isomorphic.

X	1	5	8	12
1	1	5	8	12
5	5	12	1	8
8	8	1	12	5
12	12	8	5	1

X	I	R	R''	R'
I	I	R	R'''	R'
R	R	R'	I	R'''
R'''	R'''	I	R'	R
R'	R'	R''	R	I

An isomorphism exists between the group of the square and a group of permutations of the four vertices 1, 2, 3, 4 of the square. The group table of the permutations, when compared with that of the group of the square, is isomorphic to it.

I —— I = e

R —— (1234) = a

R' —— (13)(24) = b

R" —— (1432) = c

H —— (14)(23) = d

V —— (12)(34) = f

D —— (24) = g

D' —— (13) =h

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	g	h	f	d
b	b	c	e	a	f	d	h	g
c	c	e	a	b	h	g	d	f
d	d	h	f	g	e	b	c	a
f	f	g	d	h	b	e	a	c
g	g	d	h	f	a	c	e	b
h	h	f	g	d	c	a	b	e

5. Cyclic Groups

A group, G, is cyclic if it contains some one element x whose powers exhaust G; this element is said to generate the group. The order of an element a in a group is the least positive integer m such that $a^m = e$; if no positive power of a equals the identity, a has order infinity.

The order of every element in the group of the square is either 4 or 2:

R - order 4

R' - order 2

R'' - order 4

H - order 2

V - order 2

D - order 2

D' order 2

The multiplicative group of 1, 2, 3, 4, 5, 6 mod 7 is cyclic, although not all of the elements generate the group. The smallest element whose powers exhaust the group is 3.

$3^1 = 3$ $\quad 3^3 = 6$ $\quad 3^5 = 5$

$3^2 = 2$ $\quad 3^4 = 4$ $\quad 3^6 = 1.$

The other element which generates the group is 5.

$5^1 = 5$ $\quad 5^3 = 6$ $\quad 5^5 = 3$

$5^2 = 4$ $\quad 5^4 = 2$ $\quad 5^6 = 1.$

The elements generated by two elements x and y subject to the defining relations $x^2 = y^3 = e$ and $xy = yx$ are x, y, y^2, xy, xy^2. The multiplication table is

X	e	x	y	y^2	xy	xy^2
e	e	x	y	y^2	xy	xy^2
x	x	e	xy	xy^2	y	y^2
y	y	xy	y^2	e	xy^2	x
y^2	y^2	xy^2	e	y	x	xy
xy	xy	y	xy^2	x	y^2	e
xy^2	xy^2	y^2	x	xy	e	y

6. Subgroups

Many groups are contained in larger groups. A subset S of a group is called a subgroup of G if S is itself a group with respect to the binary operation of G. In any group G, the set consisting of the identity e alone is a subgroup. The whole group G is also a subgroup of itself. Subgroups of G other than the trivial (improper) subgroups

e and G are proper subgroups.

The additive group mod 12 contains six subgroups; (1) The improper subgroup e, 0, (2) the improper subgroup of itself.

(3)

+	0	2	4	6	8	10
0	0	2	4	6	8	10
2	2	4	6	8	10	0
4	4	6	8	10	0	2
6	6	8	10	0	2	4
8	8	10	0	2	4	6
10	10	0	2	4	6	8

(4)

+	0	3	9	6
0	0	3	9	6
3	3	6	0	9
9	9	0	6	3
6	6	9	3	0

(5)

+	0	6
0	0	6
6	6	0

(6)

+	0	4	8
0	0	4	8
4	4	8	0
8	8	0	4

Among the subgroups of a given non-Abelian group G, one of the most important is its center. This is defined as the set of all elements a E G, such that ax = xa for all x E G. In the group of the square, by checking the group table, the subgroup (I, R') is found to be the center of the group. In the group of the equilateral triangle, the center is simply the improper subgroup (I).

7. Cosets

A far-reaching concept of abstract group theory is the idea that any subgroup S of a group G decomposes G into oosets.

A right coset (left coset) of a subgroup S of a group G is any set Sa (or aS) of all the right-multiples sa (left-multiples as) of the elements s of S by a fixed element a in G. If S is finite, each right coset Sa of S has exactly as many elements as S does.

The right cosets of the subgroup S = [(1)(2)(3)(4), (13)] of the group composed of (1)(2)(3)(4) = i, (1234) = a, (13)(24) = b, (1432) = c, (13) = d, (24) = e, (12)(34) = f, (14)(32) = g are

$$Si = Sd = (13)$$
$$Sa = Sg = (1234), (14)(32)$$
$$Sb = Se = (13)(24), (24)$$
$$Sc = Sf = (1432), (12)(34).$$

The left cosets are

$$iS = dS = (13)$$
$$aS = fS = (1234), (12)(34)$$
$$bS = eS = (13)(24), (24)$$
$$cS = gS = (1432), (14)(32).$$

8. Permutation Groups

A group of permutations on a finite set of elements illustrates the theory of groups well. A permutation is a one-one transformation of a finite set into itself. It is customary to describe a permutation by actually designating the image of each element under the mapping in a "two-row" notation or by a "one-row" notation for cyclic permutations in which any letter is followed by its transform and the last letter is transformed into the first. The permutation ϕ is

$1\phi = 2$, $2\phi = 3$, $3\phi = 4$, $4\phi = 5$, $5\phi = 1$ and can be written as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ or as (12345), (23451), (34512), (45123), (51234). The notation of a cyclic permutation can be extended to any permutation: any permutation ψ can be written as a product of cycles, acting on disjoint sets of symbols. If ψ is $1\psi = 3$, $3\psi = 2$, $2\psi = 1$, $4\psi = 5$, $5\psi = 4$, then ψ is the product of two cycles (132)(45). Also, the order of any permutaion ϕ is the least common multiple of the lengths of its disjoint cycles. To find the order of (abcdef)(abcd)(abc), the product of the three cycles which are not disjoint must be found. It becomes (bdefc), so the order is 5. In the permutation (abcdef)(ghi)(klm), there are three disjoint cycles with the least common multiple of the lengths of the disjoint cycles as 12, so the order is 12.

The group of the symmetries of the equilateral triangle can be expressed in terms of permutations and cycles if 1, 2, 3, represent its vertices.

I = (1)(2)(3)	R' = (123)	D = (132)
R = (23)	V = (13)	D' = (12).

The group of the square may be expressed in a similar manner as a permuatation of the 4 vertices.

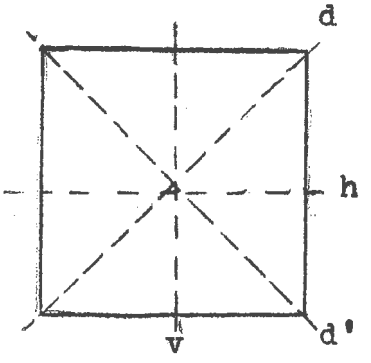
9. Homomorphism

A singled-valued transformation from a group G to a group G' which preserves multiplication but is not necessarily one-one is a homomorphism. Under any homomorphism $G \rightarrow G'$, the identity e of G goes into the identity G', and inverses into inverses. The set of all elements of G mapped on the identity

e' of G', under a homomorphism of G to G', is a subgroup of G and is known as the kernel.

In the homomorphism $n \rightarrow i^n$, where $i = \sqrt{-1}$ and $n \in z$, the kernel is all n which are multiples of four.

In a square let the two diagonals be d and d', the axes h and v. There is a homorphism $\phi \leftrightarrow \phi^*$ in which each motion ϕ in the group of the square induces a permutation ϕ^* on d, d', h, and v.



$R \leftrightarrow (dd')(hv)$ $\quad V \leftrightarrow (dd')$

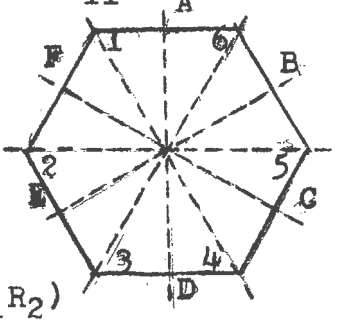
$R' \leftrightarrow I$ $\quad D \leftrightarrow (hv)$

$R'' \leftrightarrow (dd')(hv)$ $\quad D' \leftrightarrow (hv)$

$H \leftrightarrow (dd')$ $\quad I \leftrightarrow I$

In this homomorphism the kernel is (I, R').

The group of the regular hexagon obtained by six rotations and six reflections represented by $S_0, S_1, S_2, \ldots, S_{11}$ is homomorphic to a set of reflections R_0, R_1, R_2 through AD, BE, CF, respectively.



There are six two-one correspondences.

$S_0, S_3 \leftrightarrow (1)$ $\quad S_1, S_4 \leftrightarrow (R_0R_1R_2)$

$S_2, S_6 \leftrightarrow (R_0R_2R_1)$ $\quad S_6, S_{11} \leftrightarrow (R_0R_1)$

$S_7, S_{10} \leftrightarrow (R_1R_2)$ $\quad S_8, S_9 \leftrightarrow (R_0R_2)$

The kernel is (S_0, S_3).

10. Automorphisms

An isomorphism of a system S with a system S' is said to be an automorphism if S and S' are the same system. An automorphism can be thought of as a shuffling of the elements

of a system but with the operations and relations in the system remaining unaltered.

The multiplicative group made up of a, b, ab, and the identity e has the group table shown and is automorphic:

X	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$e \longleftrightarrow e$ $(=a^2 = b^2)$

$a \longleftrightarrow b$

$b \longleftrightarrow a$

$ab \longleftrightarrow ba$

The group G composed of (1), (12), (13), (23), (123), and (132) has the group table

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(123)	(132)	(13)	(23)
(13)	(13)	(132)	(1)	(123)	(23)	(12)
(23)	(23)	(123)	(132)	(1)	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	(1)
(132)	(132)	(13)	(23)	(12)	(1)	(123)

An automorphism of G exists when

$(1) \longleftrightarrow (1)$ $\qquad$ $(23) \longleftrightarrow (23)$

$(12) \longleftrightarrow (13)$ $\qquad$ $(123) \longleftrightarrow (132)$

$(13) \longleftrightarrow (12)$ $\qquad$ $(132) \longleftrightarrow (123)$.

The group tables are abstractly the same.

BIBLIOGRAPHY

Birkhoff, Garrett and Saunders MacLane. A Survey of Modern Algebra. New York: The Macmillan Company, 1965.

Fang, Joong. Abstract Algebra. New York: Schaum Publishing Co., 1963.

Moore, John T. Elements of Abstract Algebra. New York: The Macmillan Co., 1962.

Weiss, Marie J. Higher Algebra for the Undergraduate. New York: John Wiley & Sons, Inc., 1949.