1966

An Investigation of the Group and Some Simple Algebraic Systems

Helen Kelly Schaal
Central Washington University

AN INVESTIGATION OF THE GROUP AND SOME SIMPLE ALGEBRAIC SYSTEMS

A Thesis

Presented to

the Graduate Faculty

Central Washington State College

In Partial Fulfillment

of the Requirements for the Degree

Master of Education

---

by

Helen Kelly Schaal

June, 1966

APPROVED FOR THE GRADUATE FACULTY

____
Bernard L. Martin, COMMITTEE CHAIRMAN

____
Bruce Alan Robinson

____
Donald J. Murphy

With grateful acknowledgments to Dr. Bernard Martin and Mr. Bruce Alan Robinson for their patience and encouragement in my quest for mathematical knowledge, to Dr. Don Murphy for his inspiration and guidance in the field of education, and to my husband, John E. Schaal, whose understanding love enabled me to reach this goal.

Helen Kelly Schaal
June, 1966

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I

THE PROBLEM AND DEFINITIONS OF TERMS USED

William Hamilton, by abandoning the commutative law of multiplication in his development of quaternions, opened the door for the investigation of algebras distinct from the ordinary familiar system. Algebra became algebras just as, through the development of non-Euclidean systems, geometry became geometries. This plurality led to the study of the classification of algebras.

I. THE PROBLEM

Statement of the problem. Most algebraic systems commonly studied have two operations; namely, addition and multiplication. The purpose of this thesis was to study an important class of systems in which there is only one operation.

The properties of the groupoid, semigroup, monoid, quasigroup, loop, group, and abelian group will be investigated to determine which subsets of our number system are associated with each of these algebraic systems.

In order to do this it will be necessary to include a brief discussion of the early history and development of primitive number systems, including the Egyptian number system. It is hypothesized that research will disclose a universal uniformity in the structure of number languages. This study will trace the history of the discovery of our present number systems; the natural numbers, the zero, the integers, the rational and irrational numbers, and, finally, the complex numbers, and determine which of the properties of the aforementioned algebraic systems each number system possessed.

Importance of the study. The following excerpt from the Presidential Address to the British Association for the Advancement of Science given by E. W. Hobson in 1910 gives some indication of the enormous growth of mathematical knowledge during the past two centuries.

> I have said that mathematics is the oldest of the sciences; a glance at its more recent history will show that it has the energy of perpetual youth. The output of contributions to the advance of the science during the last century and more has been so enormous that it is difficult to say whether pride in the greatness of achievement in this subject, or despair at his inability to cope with the multiplicity of its detailed developments, should be the dominant feeling of the mathematician. Few people outside of the small circle of mathematical specialists have any idea of the vast growth of mathematical literature. The Royal Society Catalogue contains a list of nearly thirty-nine thousand papers on subjects of Pure Mathematics alone, which have appeared in seven hundred serials during the nineteenth century. This represents only a portion of the total output, the very large number of treatises, dissertations, and monographs published during the century being omitted (20:108-109).

Much of this knowledge has remained in the upper stratosphere of the mathematical world and has only recently begun to trickle down to the lower levels. In view of this increased knowledge, there is a need for mathematics teachers to broaden their background in order to have a more comprehensive view of their subject matter and its place in the world of today.

II. DEFINITIONS OF TERMS USED

A set and its elements are basic undefined concepts in mathematics, but the notions are intuitively very simple.

Element. An element is a thing; i.e., a. (The elements in mathematics are usually numbers but they do not need to be.)

Set. A set is a collection of distinct objects of thought or perception which are the elements of the set. A set may be indicated by listing its elements; i.e., $S = \{a, b, c\}$ where a, b, and c are the elements of set S, or we may state a property of the elements; i.e., $S = \{x \mid x$ is a counting number$\}$.

Operation. An operation is the combining of two elements of a set to produce a third element of the set. The ordinary operations of arithmetic are addition, multiplication, subtraction, and division. Because we combine two elements at a time, we call these operations "binary operations."

Commutative Law. An operation o defined on a set is said to be commutative if for any elements, a, b, of the set, a o b = b o a.

Associative Law. An operation o defined on a set is said to be associative if, for any elements, a, b, c, of the set, (a o b) o c = a o (b o c).

CHAPTER II

REVIEW OF THE LITERATURE

The first comprehensive text on groups with extensive contributions to the theory was written by Sylow, a Norwegian, and Burnside, an English mathematician, and published around 1900. Interest in group theory declined in the late thirties and early forties, but in recent years there has been a resurgence of interest and now many of the world's best mathematicians are engaged in this field of research. Many of the articles published on the subject of groups and simple algebraic systems have as yet not been fully translated into English (15:98-105).

I. LITERATURE ON SIMPLE ALGEBRAIC SYSTEMS

A book, CORPS LOCAUX, by Jean-Pierre Serre, grew out of a course of lectures at the College de France (1958-1959) and expounded on local class field theory and related subjects. The second part was about ramification and alludes to a method of Noether-Kahler as well as Dedekind's method. This book also considered Hilbert's ramification subgroups G_i of the Galois group G = G (L/K). This was followed by a short section on characters of finite groups, including Frobenius' reciprocity homomorphisms instead of monomorphisms. Galois nonabelian cohomology was used to introduce

Brauer's group. Artin's quasi-algebra "closedness" was given. This was a review of the difficult work of many mathematicians on fields and groups (32:243).

Valucé wrote in Russian on the left ideals of the semigroup of endomorphisms of a free universal algebra. No proofs were given (36:235-237).

De Carvallo and Tamari wrote that in a monoid one may consider partial associative laws A_2, A_3, ..., A_n, where A_n asserts that, for arbitrary elements a_o, a_1, ..., a_n, all bracketings of the product $a_o a_1 \ldots a_n$ that make calculation possible, lead to the same answer. A monoid is associative, if all these laws hold. The authors studied the associativity of the monoid S (M) constructed from the monoid M by adjoining a unit element and an inverse for every element and imposing the appropriate relations (16:157-169).

Čupona wrote on n-subsemigroups. If S is a semigroup, a subset $Q^n \subseteq Q$ is called an n-subsemigroup. A detailed theorem about n-subsemigroups was proved (13:5-13).

Hall wrote on simple algebraic systems, defining the quasigroup, the loop, and the semigroup. He discussed and gave an example of a quasigroup with an inverse but no unity (19:7-9).

Tamura, Merkel, and Latimer made a study of the direct product of right singular semigroups and certain groupoids. They defined right groups and showed that these groups led to the more general system "in which a weakened associative law holds." To these they applied the name M-groupoids. They proved an M-groupoid is the direct product of a right singular semigroup and a groupoid with a two-sided identity, and they showed how defining conditions for M-groupoids compared with those for right groups (34:118-123).

Tamura and Burnell made a study of the extension of semigroups with operations. Let S be a semigroup and Υ be a commutative semigroup of mono-endomorphisms of S. The authors indicated the existence of a semigroup S* and an abelian group Υ^* of automorphisms of S* such that (i) S is embedded in S*, (ii) Υ^* is the least abelian group into which Υ is embedded, and (iii) the α^* of Υ^* corresponding to α of Υ is an extension of α to S*. The proof was constructive but details were omitted. It was noted that the procedure is valid when S is a groupoid (33:495-498).

Kimura, Tamura, and Merkel wrote on semigroups in which all subsemigroups are left ideals. Terms were defined from which the following lemma was implied: If S is a λ-[p-,α -] semigroup, then any subsemigroup of S as well as any homomorphic image of S is of the same type. The idempotents of a λ -semigroup S were used to obtain a natural decomposition of S as the disjoint union of unipotent λ-semigroups. The structure of unipotent λ-semigroups and general λ -semigroups were proved and the structure theorem of

α-semigroups was shown to be an application of them (22:52-62).

Bruik defined and gave examples of groupoids, quasigroups, loops, and groups. He stated that groupoids are very common in mathematics. However, for the most part, they are not very interesting in their own right, but only with reference to topics in which they are largely unnoticed (9:61-70).

Moore, in writing of algebraic systems, also defined the group, the monoid, the semigroup, and the groupoid, and stated the properties of each system (27:189).

II. LITERATURE ON GROUPS

Group theory was first studied by Galois as permutation transformations. The objects which were permuted were the roots of an equation, and the effect on certain number fields in which these roots lay was studied (15:98-105). The work of Cauchy, Lagrange, Abel, and Galois was done from this point of view. "Galois is considered the father of group theory and this is probably the only thing he gave to posterity. He died at the age of twenty-one. He gave the name 'group' to these systems" (15:98-105).

Wilder wrote on "operations" such as those of addition and multiplication in elementary arithmetic, and also those exemplified by the combining of transformations in geometry.

He discussed how these came to be studied from an abstract point of view, and how it became apparent that there was an underlying common idea. This led to the axiomatic definition of group and to a large body of theorems which constituted "group theory" which was available for application wherever groups could be recognized as having a role in any field of mathematics (38:158-160).

Eves and Newsom wrote of finite and infinite groups. They also discussed the simpler concept of a semigroup (17:129-131).

Newman stated that the Theory of Groups is "a branch of mathematics in which one does something to something and then compares the result with the result obtained from doing the same thing to something else, or something else to the same thing" (29:1534). This is a broad definition, but Newman did not consider it trivial. However, the theory was a supreme example of the art of mathematical abstraction. It was "concerned only with the filigree of underlying relationships; it is the most powerful instrument yet invented for illuminating structure" (29:1534-1557). Nevertheless, the theory of groups has effected a remarkable unification of mathematics, revealing connections between parts of algebra and geometry that were long considered distinct and unrelated. "Whenever groups disclosed themslves or could be introduced, simplicity crystallized out of comparative chaos" (29:1534-1557).

Newman also wrote that group theory has helped physicists penetrate to the basic structure "of the phenomenal world, to catch glimpses of innermost pattern and relationship ... This is as deep as science is likely to get" (29:1534-1557).

Miller credited P. Ruffini with developing an important theorem in group theory "in which it is shown that the order of a group is divisible by the order of every one of its subgroups in a given group whose order is an arbitrary divisor of the order of the group" (26:74-95). Ruffini also developed the classification of permutation groups. However, his terminology is not used by present-day mathematicians. These classifications had approximately the same concepts of intransitive, transitive imprimitive, and transitive primitive (26:74-78).

Dean defined a group and stated its properties. He also discussed Lagrange's theorem: The number of elements in a finite group is divisible by the number of elements in any of its subgroups. (Note: the number of elements in the group or subgroup is its order.) Therefore, the order of a group is divisible by the order of every one of its subgroups (15:98-105).

Litvak stated that for many years the axiom of commutativity was assumed. It was W. R. Hamilton, the great Irish mathematician, who constructed a system of algebra in which the commutative law is denied. This discovery pointed out the basic nature of this law. Groups which satisfy the commutative law are called Abelian (24:30-32).

CHAPTER III

NUMBER SYSTEMS

It is impossible to name the exact period in which number words originated because there is unmistakable evidence that it preceded witten language by many thousands of years. The original meaning of number words was lost in antiquity probably because the names of the concrete objects from which the number words derived their names have undergone a complete metamorphosis. But while time has brought about radical changes in language, the number vocabulary has virtually remained unchanged. Figure 1 shows the extraordinary stability of number words.

I. PRIMITIVE AND EARLY NUMBER SYSTEMS

A near universality in the selection of the base of the various number systems is found. In all Indo-European languages, the base of numeration is ten; that is, the first ten number words are independent. A compounding principle is used up to 100. All languages have independent words for 100 and 1000 (14:12).

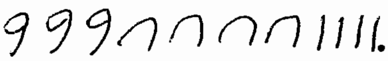
In the Egyptian hieroglyphic notation digits from one to nine were represented by vertical strokes; for example, four would be written ||||. Multiples of ten were represented by "croquet wickets," so that forty would be written

NUMERAL	SANSKRIT	ANCIENT GREEK	LATIN	GERMAN	ENGLISH	FRENCH	RUSSIAN
1	eka	en	unus	eins	one	un	odyn
2	dva	duo	duo	zwei	two	deux	dva
3	tri	tri	tres	drei	three	trois	tri
4	catur	tetra	quator	vier	four	quatre	chetyre
5	ponca	pente	quinque	funf	five	cinq	piat
6	sas	ex	sex	sechs	six	six	shest
7	sapta	epta	septem	sieben	seven	sept	sem
8	asta	octo	octo	acht	eight	huit	vosem
9	nava	ennea	novem	neun	nine	neuf	deviat
10	daca	deca	decem	zehn	ten	dix	desiat
100	cata	ecatron	centum	hundert	hundred	cent	sto
1000	sehastne	xilia	milia	tausend	thousand	mille	tysiaca

(14:12-18)

FIGURE 1

NUMBER WORDS

. The number 344 was represented hieroglyphically as . Large numbers in the hundreds of thousands appeared in this notation at the time the pyramids were built. However, both the Ahmes and Moscow papyri used a very different notation, a more cursive script known as "hieratic" which abbreviated the older method by using a new collection of symbols. The new method used a distinctive mark for each of the first nine multiples of integral powers of ten (8:127-128).

In addition to the decimal system, two other bases were fairly wide spread. These two other systems were the quinary, base 25, and the vigesimal, base 20. However, their character "confirms to a remarkable degree the anthropomorphic nature of our counting scheme" (14:13). Many languages bear a trace of a quinary system, and it is believed that some decimal systems passed through the quinary stage (14:13).

II. BASIC NUMBER SYSTEMS

The natural, or counting, numbers originated in man's desire to keep records of his goods and his flocks. Archeological researches traced such records to the caves of prehistoric man. The oldest records of a systematic use of written numerals were those of the Sumerians, Egyptians, and Chinese. These were all traced back to the same era, around

3500 B.C. (14:21). The set of natural, or counting, numbers is designated as $N = \{1, 2, 3, 4, 5, 6, \ldots\}$.

Little progress was made in mathematical calculation, however, until an unknown Hindu discovered the <u>principle of position</u>. But there was still one difficulty. There was no symbol for an empty column. "The concrete mind of the ancient Greeks could not conceive the void as a number" (14:31). Neither did the unknown Hindu consider zero the symbol for nothing (14:35).

The Indian <u>sunya</u>, which meant <u>empty</u> or <u>blank</u> had no connotation of "void" or "nothing." It was the Arabs of the tenth century who, when they adopted the Indian numeration, translated the India <u>sunya</u> to their own <u>sifr</u> which meant <u>empty</u> in Arabic. When introduced into Italy, <u>sifr</u> was latinized into <u>zephirum</u> which eventually culminated in the Italian <u>zero</u>. When Jordanus Nemeraruis introduced the Arabic system into Germany, he kept the Arabic word but changed it slightly to <u>cifra</u>. Anglicized <u>cifra</u> became <u>cipher</u> but retained its original meaning of <u>zero</u>. In the history of civilization the discovery of zero stands out as one of the greatest achievements of the human race (14:35).

Some authors designate the set of natural numbers and zero as the "whole numbers," i.e., $W = \{0, 1, 2, 3, \ldots\}$.

The discovery of the negative numbers is unknown. However, it was known that they were first used in India in the early centuries after the birth of Christ. The Hindus had symbols for the negative numbers which were different from those used today (14:81).

The positive and negative counting numbers and zero are designated the "integers," i.e., $I = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.

The discovery of fractions is lost in antiquity. According to Aristotle, mathematics originated because the priestly class of Egypt had the leisure time needed to study. Two thousand years later this statement was corroborated by the discovery of a papyrus, now treasured in the Rhind collection at the British Museum. This document was written by Ahmes, who lived before 1700 B.C., and is called "directions for knowing all dark things." The work is a collection of problems in geometry and arithmetic and is much concerned with the reduction of fractions to a sum of fractions each of whose numerators is unity (34:2).

The fractions, which include the integers, since they can be put in fractional form with unity as the denominator, are designated the "rational numbers" and are written $Ra = \{a/b \in Ra \mid a \text{ and } b \text{ are integers, except that } b \neq 0\}$ (14:102).

The attempt to apply rational numbers to problems in geometry resulted in a crisis in mathematics. The determination of the diagonal of a square and the circumference of a circle revealed new entities not found in the rational domain. Pythagoras made approximations of the square root of integers, but Archimedes made the first systematic application of the principle (35:13-15).

In 1872, Richard Dedekind used the idea of partition, "a manner of severing a line into two mutually exclusive complementary regions" (14:141). The essence of the Dedekind concept is contained in a passage in the Appendix of this thesis. It was taken from his essay "Continuity and Irrational Numbers" which appeared in 1872.

These new entities not found in the rational domain are called irrational numbers. The early Greeks demonstrated the need for such numbers as follows: If each side of a square is one inch long, we know by the theorem of Pythagoras that the length x of the diagonal is given by the equation $x^2 = 1^2 + 1^2$, or $x^2 = 2$. This means that x equals the square root of 2. Since the diagonal has a definite length, the square root of 2 must be a definite number. It can be shown by the usual indirect method of proof that $\sqrt{2}$ cannot be expressed as the quotient of two integers and, therefore, is not a rational number (35:13-15).

The system of numbers containing both the rational and irrational numbers is designated the real numbers and is written $Re = \{x \in Re \mid x \text{ is a rational number or } x \text{ is an irrational number}\}$.

Girolamo Cardan, who opened up the general theory of the cubic and quartic equations by discussing the number of roots an equation may have, surmised the need not only for negative but for complex (or imaginary) numbers to effect complete solutions (35:64-65). To make possible the operation of expressing even roots of negative numbers, mathematicians invented numbers like $\sqrt{-1}$, $\sqrt{-3}$, etc., which are called "imaginary" numbers. Therefore, an imaginary number is an indicated square root of a negative number. It follows that any even root of a negative number is imaginary. A complex number is a number having the form (a + bi) where a and b are real numbers and i is the imaginary unit $\sqrt{-1}$ (35:64).

CHAPTER IV

SIMPLE ALGEBRAIC SYSTEMS

The simple algebraic systems considered in this thesis are the groupoid, the semigroup, the monoid, the quasigroup, and the loop. The literature on the various simple algebraic systems was somewhat limited to the writer, and the writers on the subject lacked a consensus of opinion on definitions and properties. For instance, A. H. Clifford and H. B. Mann investigated a semigroup G which satisfied the two axioms:

1. There is at least one (left identity) e in G such that ea = a for all a in G.

2. For every a in G and for every left identity e in G, there is at least one b in G such that ab = e (34:118).

Clifford called such systems <u>multiple groups</u>, and Mann called them (l, r) systems. Tamura, Merkel, and Latimer in <u>The Direct Product of Right Singular Semigroups and Certain Groupoids</u> referred to the same semigroups as <u>right groups</u> (34:118). Because of the lack of agreement on the subject, only the general definition and basic properties of each will be investigated.

I. THE GROUPOID

A groupoid is a non-empty set of elements S on which a binary operation o has been defined and subject only to the axiom: If a, b are any elements belonging to set S, then a o b is also an element belonging to S and a o b is unique (9:61).

This is known as the Closure Postulate which has great significance not only in groupoids but also in many other algebraic systems (9:61).

Let us now examine our number systems to determine whether or not they are groupoids.

The natural numbers under the operations "multiplication" and "addition" are groupoids since ab = c; example, 2 x 3 = 6, and a + b = c; example, 2 + 3 = 5 for all a, b, c in N.

The set of natural numbers with zero constitute groupoids under operations of "multiplication" and "addition."

Examples: ab = c or 2 x 0 = 0
and a + b = c or 2 + 0 = 2

and, therefore, the Closure Postulate applies.

The set of integers, under the same two operations, are groupoids since (-2) (-3) = 6 and (-2) + (-3) = -5 for all a, b contained in the set of integers and the set is closed under both operations.

Also, upon examination, both the rational and the real number systems are groupoids according to the definition, and in all these cases the result of the operation upon two elements is unique and the set is closed.

II. THE SEMIGROUP

A semigroup is a groupoid subject to the following postulate: For arbitrary elements a, b c belonging to set S, a o (b o c) = (a o b) o c. This is the Associative Postulate.

Now if the set of natural numbers was considered together with the operation "multiplication" or the operation "addition," the Associative Postulate holds (27:189).

Examples:

$$2 \times (3 \times 4) = (2 \times 3) \times 4 \quad \text{and} \quad 2 + (3 + 4) = (2 + 3) + 4$$
$$2 \times (12) = (6) \times 4 \qquad\qquad 2 + (7) = (5) + 4$$
$$24 = 24 \qquad\qquad 9 = 9$$

Therefore, the set of natural numbers under the operation "multiplication" and under the operation "addition" is a semigroup.

On examination the natural numbers and zero, the integers, the rational numbers, and the real numbers are found to be semigroups. It follows that <u>every</u> semigroup is a groupoid and each groupoid mentioned in the preceding section is a semigroup. Are all groupoids, therefore, semigroups? No. We can find examples of groupoids that are not semigroups but not among the basic number systems.

Example I. $S = \{x \mid x \text{ is a positive real number.}\}$ and $a \circ b = a^b$, $a, b \in S$.

Example II. $S = \{x \mid x \text{ is a positive real number.}\}$ and $a \circ b = |a - b|$, where $|x|$ denotes the absolute value of x, and $a, b \in S$.

In example I, $(2 \circ 2) \circ 3 = 4 \circ 3 = 64$,
but $2 \circ (2 \circ 3) = 2 \circ 8 = 256$.

In example II, $(1 \circ 2) \circ 3 = 1 \circ 3 = 2$,
but $1 \circ (2 \circ 3) = 1 \circ 1 = 0$ (9:61).

These examples suggest that we have been "dealing with groupoids for years and have been getting along quite nicely without the Associative Law" (9:61).

III. THE MONOID

The monoid is a semigroup with the following property: There exists in set S a unique element e such that $a \circ e = e \circ a = a$ for all a in S (29:189).

In examining the basic number systems, it is found that the set of natural numbers under the operation "multiplication" is a monoid as it has the identity element "1". However, under the operation "addition," there is no identity element and, therefore, the set of natural numbers would not be a monoid.

The remaining basic number systems are monoids under either operation "multiplication" or "addition," because of the fact that the natural numbers form a subset of these systems.

An example of a semigroup that is not a monoid is the set of integers, modulo 4, under multiplication. The identity element for "2" is missing.

IV. THE QUASIGROUP

A quasigroup is a groupoid which satisfies the following postulates:

1. If a, b are elements in S, there is one and only one x in S such that a o x = b.

2. If a, b are in S, there is one and only one y in S such that y o a = b (9:62).

The requirement that x and y be unique cannot be omitted (9:62).

Sometimes these postulates are combined with the Closure Postulate into one postulate as follows:

> If any two x, y, z are given as elements of S, the equation x o y = z uniquely determines the third as an element of S (9:62).

Under the operations of "multiplication" and "addition" the basic number systems are quasigroups. However, the example given previously where $a \circ b = |a - b|$ is not a quasigroup.

Example: If $5 \circ x = 2$
then $|5 - x| = 2$
$x = 3$
or $x = 7$

Therefore, x is not unique in the equation.

An interesting example of a quasigroup with an inverse property but no unity is given by Marshall Hall, Jr.:

> We call a system with a binary product and unary inverse satisfying $a^{-1}(ab) = b = (ba)a^{-1}$ a quasigroup with the inverse property, this law being the inverse property. We must show that the product defines a quasigroup.

If $ab = c$, we find $b = a^{-1}(ab) = a^{-1}c$, and $a = (ab)b^{-1} = cb^{-1}$. Thus, a and b determine c uniquely; and also given c and a, there is at most one b, and given c and b, there is at most one a.
Write $a(a^{-1}c) = w$.
Then $a^{-1}[a(a^{-1}c)] = a^{-1}w$, whence $a^{-1}c = a^{-1}w$.
Then $(a^{-1})^{-1}(a^{-1}c) = (a^{-1})^{-1}(a^{-1}w)$, whence $c = w$.
Hence $a(a^{-1}c) = c$, and similarly, $(cb^{-1})b = c$ and the system is a quasigroup. We note that an inverse quasigroup need not be a loop. With three elements a, b, c, and relations $a^2 = a$, $ab = ba = c$, $b^2 = b$, $bc = cb = a$, $c^2 = c$, $ca = ac = b$, we find that each element is its own inverse, and we have a quasigroup with the inverse property and no unit (19:7-9).

V. LOOP

A loop is a quasigroup that satisfies the following axiom: If a is an element in S, there exists an element e in S such that $a \circ e = a = e \circ a$ for each a in S (9:62). The identity element e is unique when it exists (9:63).

The basic number systems are loops under the operation "multiplication," and all, but the set of natural numbers, are loops under "addition" since the additive identity is "0."

VI. SUMMARY

In this chapter simple algebraic systems such as the groupoid, semigroup, monoid, quasigroup, and the loop have been discussed with appropriate definitions and postulates. The writer has endeavored to give examples which demonstrate the various algebraic systems and the differences between them.

CHAPTER V

THE GROUP

The theory of groups is an important part of algebra and many articles and books have been written on the subject. In this chapter will be presented only a few of the fundamental properties of groups and our basic number systems will be examined relative to these properties. Some other examples which will illustrate the wide range of applications of the theory will also be given.

I. HISTORY OF GROUP THEORY

During the early part of the nineteenth century, theory of groups, as a distinct branch of algebra, developed as the theory of finite substitution groups to fill the needs of Galois' theory. Abel used this theory of substitution groups to prove that it is impossible to solve, algebraically, equations higher than the fourth degree. The theory was then generalized to the study of properties of a single operation defined on a set of a finite number of elements. Arthur Cayley in 1854 was the first to discuss the theory from an abstract point of view. L. Kronecker in 1870 and H. Weber in 1888 formulated the earliest explicit sets of axioms for a group (24:30-32).

The end of the nineteenth century and the first decade of the twentieth century is called "the golden age of the theory of finite groups" (24:30-32). The theory acquired all the essential features it has today during this period. Some of the mathematicians who helped in this development were G. Frobenius (1849-1917), O. Holder (1859-1937) W. Burnside (1852-1927), and G. A. Miller (1863-1951) (24:30-32).

The commutative axiom had been assumed for many years when W. R. Hamilton constructed an algebraic system in which this axiom was denied. Today, groups which satisfy the commutative axiom are called abelian. They are named after Abel the Norwegian mathematician (24:30-32).

The restriction of "finiteness" of a group had to be removed before group theory could be extended to many branches of mathematics, such as the theory of numbers, topology, and the theory of automorphic functions (24:30-32).

Infinite abelian groups were developed during the years between 1930 and 1950, and a great many results were discovered. However, the mathematical world had to overcome opposition to the concept of infinity before this could take place. One of the greatest mathematicians of all time, C. F. Gauss, said in answer to an idea of H. C. Schumacker, "I protest . . . against using infinite magnitude as something consummated; such a use is never admissible in mathematics. The infinity is only a façon de parler. One has in mind limits which certain ratios approach as closely as is desirable while other ratios may increase indefinitely." Cantor fought against this attitude and was successful in refuting it (24:30-32).

II. DEFINITION OF A GROUP

A group is a nonempty set G on which there is defined a binary operation "o" and which satisfies the following properties:

1. For every a, b in G, a o b is an element of G. (closure property)
2. For every a, b, c in G, (a o b) o c = a o (b o c). (associative axiom)
3. For every a in G, there exists an element e in G such that a o e = e o a = a. (identity axiom)
4. For every a in G, there exists an element x in G such that a o x = x o a = e. (inverse axiom) (25:167)

A group, then, is a monoid which also satisfies the fourth axiom listed above. We can, also, define a group as a loop which also satisfies both the second and fourth axioms.

III. BASIC NUMBER SYSTEMS

The set of natural numbers, with the operation "addition", is not a group. In this case, the identity and the inverse is missing.

The set of natural numbers, with operation "multiplication", is not a group. The closure axiom holds since a o b is in N. The second axiom holds since (a o b) o c =

a o (b o c) for all a, b, c in N. In this case, the identity of the group is 1 since a o 1 = 1 o a = a for all a in N. However, the inverse of the element "a" is not in the group.

The set of natural numbers and zero, with the operation "addition," is not a group. In this case the identity "0" is an element of the set but the inverse of "a" is missing.

The set of natural numbers and zero, under the operation "multiplication," is not a group since the inverse of "a" is missing.

The set of integers, under the operation "addition," is a group. Under this operation the set is closed since a o b is in G. The associative axiom holds since (a o b) o c = a o (b o c) for all a, b, c in G. The identity of the group is "0" since 0 o a = a o 0 = a for all a in G. The inverse of the element a is the element ¯a since a o (¯a) = ¯a o a = 0. This group is frequently called the additive group of integers.

The set of integers with operation "multiplication" is not a group. Both the closure and associative axioms hold and the identity "1" is an element of the set but the inverse of "a" is missing.

The set of rational numbers under "addition" is a group with all axioms holding.

The set of rational numbers under "multiplication" is not a group since there is no multiplicative inverse for "0".

It follows that the set of real numbers under operation "addition" is a group and under the operation "multiplication" is not a group.

Many writers define the inverse postulate as follows: There exists an element x in G such that a o x = x o a = e for all a in G except perhaps for zero (33:125).

If we use this definition of the inverse instead of the former one, both the set of rational and the set of real numbers, under the operation of "multiplication", are groups.

IV. THE ABELIAN GROUP

All the aforementioned basic number systems that constitute groups have an additional property not required by the definition of a group. This additional property is the commutative axiom which may be stated as follows: If a, b is in G, then a o b = b o a.

A group which satisfies this additional axiom is called an "abelian" or "commutative" group. There are many important non-abelian groups of which the permutation group is an example (25:169).

V. THE PERMUTATION GROUP

The concept of a permutation is the process of replacing each element of a finite set by an element (not necessarily a different one) chosen from the same set.

Starting with the elements 1, 2, 3, ..., n, and replacing these, respectively, by j_1, j_2, j_3, ..., j_n, where $j_i \in$ positive integers less than or equal to n and $j_i \neq j_k$, this permutation is indicated by the following notation:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

since j_1 replaces 1, j_2 replaces 2, j_3 replaces 3, and j_n replaces n (37:42-44).

To multiply permutations the single permutation is found, which results by performing two replacements, one after the other, for example:

The result of multiplying $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$ by $\begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}$ is the product $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}$ where k_1, k_2, k_3, ..., k_n are 1, 2, 3 ..., n in some order (37:42-44).

The number of possible **permutations** on n elements of any set is n!(37:42-44).

To demonstrate that the permutation of the elements of a finite set form a group, but a nonabelian group, under permutation multiplication, the group properties are discussed below.

1. The closure postulate holds since the product of two permutations is another permutation on the same elements.

2. The associative postulate holds, because, given the following permutation, $p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$, $q = \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}$, and $r = \begin{pmatrix} k_1 & k_2 & k_3 & \cdots & k_n \\ m_1 & m_2 & m_3 & \cdots & m_n \end{pmatrix}$ where m_1, m_2, ..., m_n are the integers 1, 2, ..., n in some order, $p \circ q =$

$\begin{pmatrix} 1 & 2 & 3 & \ldots n \\ k_1 & k_2 & k_3 & \ldots k_n \end{pmatrix}$ and $(p \circ q) \circ r = \begin{pmatrix} 1 & 2 & 3 & \ldots n \\ m_1 & m_2 & m_3 & \ldots m_n \end{pmatrix}$ while $qr = \begin{pmatrix} j_1 & j_2 & j_3 & \ldots j_n \\ m_1 & m_2 & m_3 & \ldots m_n \end{pmatrix}$ and $p\ (qr) = \begin{pmatrix} 1 & 2 & 3 & \ldots n \\ m_1 & m_2 & m_3 & \ldots m_n \end{pmatrix}$.
Therefore $(pq)r = p\ (qr)$, where pq has the same meaning as $p \circ q$.

3. The identity is

$$i = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

for it obviously has the property $ip = pi = p$ for any permutation p on the n integers 1, 2, ..., n.

4. The inverse of p is

$$p^{-1} = \begin{pmatrix} j_1 & j_2 & j_3 & \ldots j_n \\ 1 & 2 & 3 & \ldots n \end{pmatrix}$$

for $pp^{-1} = p^{-1}p = i$. (37:42-44).

Therefore, all the postulates for a group are satisfied.

In general this multiplication is not commutative, for if, for example, in the permutation group with three elements,

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ and } q = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

then

$$p\ q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ and } qp = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Therefore, $pq \neq qp$ and the permutation group is nonabelian.

VI. THE CYCLIC GROUP

The definition of a cyclic group is as follows:

If a group G contains an element a such that every element of G is of the form a^m for some integer m, we say that G is a <u>cyclic group</u> and that G is generated by a or that a is the generator of G (25:181).

If G is a cyclic group generated by a, then G is closed under multiplication as a^k is an element of G for every positive integer k. The associative postulate holds since $a^i (a^j a^k) = (a^i a^j) a^k$. The inverse of a^k is a^{-k}; therefore, the inverse exists for every positive integer k. Finally, a^0 is the identity of G by definition, and it follows that $G = \{a^k \mid k \text{ is an integer}\}$. Each element of a group G, therefore, can generate a cyclic sub-group of G (25:181-182).

Since $a^i a^j = a^j a^i$ for arbitrary integers i and j, it follows that a cyclic group is abelian (25:182).

VIII. SUMMARY

In this chapter the basic number systems have been investigated relative to the definition of a group. The abelian group has been investigated, and it has been shown that the permutation group is nonabelian and the cyclic group is abelian.

CHAPTER VI

SUMMARY

This was a study of an important class of algebraic systems in which there is only one operation. The properties of the groupoid, semigroup, monoid, quasigroup, loop, group, and abelian group were investigated to determine which subsets of our number system are associated with each of these algebraic systems. A brief discussion of the history and development of number systems was included.

The groupoid was the simplest algebraic system considered in this thesis. It consists of a nonempty set that satisfies the closure postulate and has one operation defined on it. All the basic number systems are groupoids under either the operation "addition" or "multiplication."

The semigroup is a groupoid that satisfies the associative postulate. All the basic number systems are semigroups under either "addition" or "multiplication."

A monoid is a semigroup that satisfies the identity postulate. Under "multiplication" all the basic number systems are monoids. Under "addition" all the basic number systems, except the natural numbers, are monoids.

A quasigroup is a groupoid which satisfies the following postulate:

> If any two x, y, z are given as elements of S, the equation x o y = z uniquely determines the third as an element of S.

All the basic number systems are quasigroups.

A loop is a quasigroup with an identity element. Therefore, under "addition" all the basic number systems, except the natural numbers, are loops. Under "multiplication" all basic number systems are loops.

The group is a monoid with an inverse element. The group may also be defined as a loop with the addition of an inverse element and the associative postulate. Under "addition" the integers, and the rational, and the real number systems are groups. Under "multiplication" none of the basic number systems are groups, unless we accept the definition of a group which does not require an inverse for the element "0". In this case, both the rational and real number systems are groups.

An abelian group is a group in which the commutative postulate holds. All the basic number systems that are groups are also abelian groups.

The hierarchal order of the simpler algebraic systems investigated in this thesis together with the group and abelian group are illustrated in Figure 2.

The process of replacing each element of a finite set by an element (not necessarily a different one) chosen from the same set is known as a permutation. Permutations under

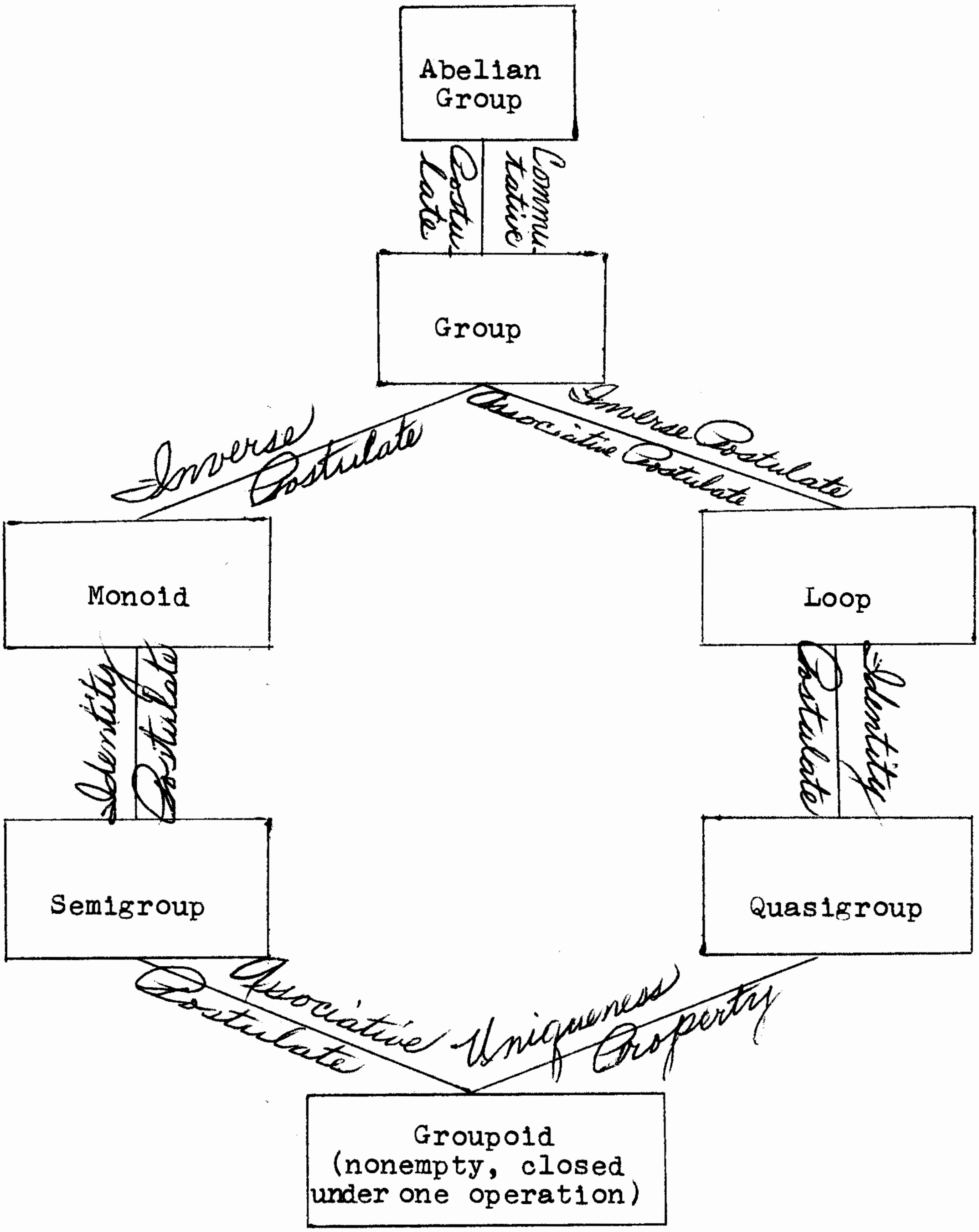


FIGURE 2

HIERARCHAL ORDER OF SIMPLE ALGEBRAIC SYSTEMS,
THE GROUP AND ABELIAN GROUP

"permutation multiplication" constitue a group, but not an abelian group since the commutative postulate does not hold.

A cyclic group is a subgroup generated by an element a of a group such that each element of the subgroup is of the form a^k, where k is an integer. The cyclic group is abelian since $a^i a^j = a^j a^i$ for arbitrary integers i and j.

There are many other types of simple algebraic systems such as M-groupoids and semigroups in which all subsemigroups are left ideals as well as other groups such as Hamiltonian groups, Mathieu groups, and continuous and discontinuous transformation groups as investigated by Sophius Lie (26:74). Dickson contributed to group theory in the areas of linear groups, hypo-abelian groups, abstract simple groups, and isomorphisms of linear groups (26:74). Any one or more of these would make the subject for a further thesis.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Albert, A. A., (ed.) Studies in Modern Algebra, Vol. 2. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1963.

2. Banks, J. Houston. Elements of Mathematics. Boston: Allyn and Bacon, Inc., 1956.

3. Bell, Eric Temple. Development of Mathematics. New York: McGraw-Hill Company, 1940.

4. Bell, Eric Temple. Mathematics, Queen and Servant of Science. New York: McGraw-Hill Company, 1951.

5. Bell, Eric Temple. The Magic of Numbers. New York: McGraw-Hill Company, 1946.

6. Bell, Eric Temple. The Handmaiden of the Sciences. Baltimore: The Williams and Wilkins Company, 1937.

7. Birkhoff, Garrett, and Saunders MacLane. A Survey of Modern Algebra. New York: The MacMillon Company 1953.

8. Boyer, Carl B. "Note on Egyptian Numeration," The Mathematics Teacher, Vol. LII, 2:127-129, February, 1959.

9. Bruik, R. H. "What is a Loop?" Studies in Modern Algebra, ed. A. A. Albert. Englewood Cliffs, New Jersey, 1963.

10. Burnside, W. Theory of Groups of Finite Order, 2nd ed. Dover Publications, Inc., Cambridge University Press, 1911.

11. Churchill, Ruel. Complex Variables and Applications, 2nd ed. New York: McGraw-Hill Book Company, Inc., 1960.

12. Cooley, R. H., and others. Introduction to Mathematics. Boston: Houghton Mifflin Company, 1937.

13. Čupona, Górgi. "On N-Subsemigroups," Bulletin on Soc., Math. and Phys. Macédoine (Macedonian English Summary), 1961. 12 (1961) 5-13 (1963). Mathematical Reviews, Vol. 27, 1964.

14. Danzig, Tobias. Number, The Language of Science. New York: The MacMillan Company, 1930.

15. Dean, Richard. "Group Theory for School Mathematics," The Mathematics Teacher, Vol. LV, 2:98-105, February, 1962.

16. De Corvallo, J. B. and Dov. Tomari. "Sur l'associativité Partielle des Symétrisotions de Semigroupes," Portugal. Mathematics, 21:157-169 (1962). Mathematical Reviews, Vol. 27, 1964.

17. Eves, Howard, and Carroll M. Newsom. The Foundations and Fundamental Concepts of Mathematics. New York: Rinehart and Company, Inc., 1958.

18. Freund, John E. A Modern Introduction to Mathematics. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1956.

19. Hall, Marshall. The Theory of Groups. New York: The MacMillan Company, 1959.

20. Hobson, E. W. "Presidential Address, British Association for the Advancement of Science," Nature, 84:285 (London, 1910).

21. Jones, Burton W. Elementary Concepts of Mathematics. New York: The MacMillan Company, 1947.

22. Kimura, Naoki, Takayuki Tamura, and Rudolph Merkel. Semigroups in Which All Subsemigroups are Left Ideals. The Canadian Journal of Mathematics, Vol. 17, pp. 52-62, 1965.

23. Kline, Morris. "The Ancients Versus the Moderns, a New Battle of the Books," The Mathematics Teacher, Vol. LI, 16:418-427, October, 1958.

24. Litvak, Barry. "History of Group Theory Leading to the Development of Infinite Abelian Groups," The Mathematics Teacher, Vol. LVI, 1:30-32, January, 1964.

25. McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960.

26. Miller, G. H. "The Evolution of Group Theory," The Mathematics Teacher, Vol. LVII, 1:26-30, January, 1964.

27. Moore, John. Elements of Abstract Algebra. New York: The MacMillan Company, 1962.

28. Moritz, Robert. Memorabilia Mathematica. New York: The MacMillan Company, 1914.

29. Newman, James R. The World of Mathematics, Vol. 3, New York: Simon and Schuster, 1956.

30. Room, T. G. "A Groupoid of Involuntary Matrices with Eight Generators," Eight Studies in Mathematics, University of Washington Publications in Mathematics, Vol. 3, 21:89-98, September, 1952.

31. Serre, Jean-Pierre. "Corps locoux," Publications de l' Institut de Mathematique de l'Universite de Moncago, Vol. VIII, Actualities Science Induct. No. 1296. Hermann, Paris, 1962, pp. 243, 36 N. F. Mathematical Reviews, Vol. 27, 1964.

32. Stabler, E. R. An Introduction to Mathematical Thought. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 1959.

33. Tamura, Takayuki, and Donald G. Burnell. "A Note on the Extension of Semigroups with Operations," Proc. Japan Acad. 38, pp. 495-498, 1962.

34. Tamura, Takayuki, R. B. Merkel, and J. F. Latimer. The Direct Product of Right Singular Semigroups and Certain Groupoids. Reprinted from the Proceedings of the American Mathematical Society, Vol. 14, 1:118-123, February, 1963.

35. Turnbull, Herbert Westren. The Great Mathematicians. New York: Simon and Schuster, 1962.

36. Valucé, I. I. "Left Ideals of a Semigroup of Endomorphisms of a Free Universal Algebra," Dokl. Akad. Nouk SSSR 150 (1963) pp. 235-237, Mathematical Reviews, Vol. 27, 1964.

37. Weiss, Marie J. Higher Algebra. New York: John Wiley and Sons, Inc., 1956.

38. Wilder, Raymond L. Introduction to the Foundations of Mathematics. New York: John Wiley and Sons, Inc., 1952.

APPENDIX

APPENDIX

THE DEDEKIND CUT

A Theory of Irrationals

Tobias Danzig, in Number, The Language of Sciences, gave the essence of the Dedekind concept which follows. The direct quotations in the passage were taken from Dedekind's essay "Continuity and Irrational Numbers" which appeared in 1872.

> "The straight line is infinitely richer in point-individuals than the domain of rational numbers is in number-individuals...
>
> "If then we attempt to follow up arithmetically the phenomena which govern the straight line, we find the domain of rational numbers inadequate. It becomes absolutely necessary to improve this instrument by the creation of new numbers, if the number domain is to possess the completeness, or, as we may as well say now, the same continuity, as the straight line ...
>
> "The comparison of the domain of rational numbers with a straight line has led to the recognition of the existence of gaps, of a certain incompleteness or discontinuity, in the former; while we ascribe to the straight line completeness, absence of gaps, or continuity. Wherein then does this continuity consist? Everything must depend on the answer to this question, and only through it shall we obtain a scientific basis for the investigation of all continuous domains. By vague remarks upon the unbroken connection in the smallest part, nothing, obviously, is gained; the problem is to indicate a precise characteristic of continuity that can serve as a basis for valid deduction. For a long time I pondered over this in vain, but finally I found what I was seeking. This discovery will perhaps be differently estimated by different people; the majority may find its substance very commonplace. It consists in the following. In the preceding section attention was called to the fact that every point of the straight line

produces a separation of it into two portions such that every point of one portion lies to the left of every point of the other. I find the essence of continuity in the converse, i.e., in the following principle;

"If all points of a straight line fall into two classes, so that every point of the first class lies to the left of every point of the second class, then there exists one and only one point which produces this division of all points into two classes, this severing of the straight line into two portions.

"As already said, I think I shall not err in assuming that every one will at once grant the truth of this statement; moreover, the majority of my readers will be very much disappointed to learn that by this commonplace remark the secret of continuity is to be revealed. To this I may say that I am glad that every one finds the above principle so obvious and so in harmony with his own ideas of a line; for I am utterly unable to adduce any proof of its correctness, nor has any one else the power. The assumption of this property of the line is nothing else than an axiom by which we define its continuity. If space has a real existence at all, it is <u>not</u> necessary for it to be continuous; many of its properties would remain the same even were it discontinuous. And if we knew for certain that space was discontinuous, there would be nothing to prevent us, in case we so desired, from filling up its gaps in thought, and thus making it continuous; this filling-up would consist in the creating of new point-individuals, and this would have to be effected in accordance with the above principle."

Dedekind views the real numbers as generated by the power of the mind to classify rational numbers. This classification he calls <u>schnitt</u>, a term translated as the <u>Dedekind cut</u>, <u>split</u>, <u>section</u>, and <u>partition</u>.

This partition is the counterpart of the Dedekind concept used in defining the continuity of the line. "Every real number constitutes a means for splitting all rational numbers into two classes which have no element in common, but which together exhaust the entire domain of rational numbers."

Conversely, any process which is capable of effecting this split in the domain of rational numbers is <u>ipso facto</u> identified with a number. By definition this is a real number, an element of the new domain.

The rational numbers are part of this domain and for any given rational number, say five, all rational numbers can be divided into two classes: those less than or equal to five go into the lower class, those greater than five go into the upper class. The two classes have no elements in common but "together they exhaust the whole set of rational numbers." The number five may be regarded as the partition and is, therefore, a real number. However, Dedekind believed this principle can be carried farther. "We can partition all rational numbers into those whose square is less than or equal to a given rational number, say two, and those whose square is greater than two. These two classes are also mutually exclusive, and, also taken together they exhaust all rational numbers. This partition too defines a real number which is identified as $\sqrt{2}$."

"While both rational and irrational numbers can be identified by partitions, the fact that it was the rational numbers that were used should be noted. There is a difference between the cases of the rational and irrational partitions. The rational partition is part of the lower class. But the irrational partition is completely ex parte and belongs to neither upper or lower class. In the rational case, the lowest class has a greatest element and the upper no least; in the irrational case, the lower class does not have a greatest element, nor does the upper class have a least" (14:172).