SUGGESTED MATHEMATICS ENRICHMENT
TOPICS FOR HIGH SCHOOL SENIORS

By

HIRAM DREXEL JOHNSTON

Bachelor of Science
Oklahoma State University
Stillwater, Oklahoma
1963

Specialist in Education
Oklahoma State University
Stillwater, Oklahoma
1969

Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
July, 1970

SUGGESTED MATHEMATICS ENRICHMENT
TOPICS FOR HIGH SCHOOL SENIORS

Thesis Approved:

Gerald K. Goff
Thesis Adviser

W Ware Marsden

Robert L Brown

Douglas B. Aichele

D. Durham
Dean of the Graduate College

ACKNOWLEDGEMENTS

The writer wishes to express his deep appreciation to all who have helped in the preparation and writing of this dissertation. Particular gratitude is due Dr. Gerald K. Goff, my dissertation advisor, who not only made valuable suggestions concerning this paper, but also for his continued interest, effort, and assistance throughout my graduate study at Oklahoma State University. Special thanks also go to Dr. Ware Marsden, my committee chairman; to Dr. Robert Brown and Dr. Douglas B. Aichele, members of my advisory committee, for their suggestions and general assistance in the preparation of the written report.

Finally, special gratitude is extended to my wife, Carol Ann, and children, Keven, Kregg, and Kournety for their understanding and encouragement throughout my graduate work.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

For several years the traditional mathematics curriculum has been under close examination and revision. Though suggestions for improvement have been diverse, some degree of agreement has been evolved on the content of the secondary school mathematics program. At the present there is generally an outline agreement on the curriculum through grade eleven. However, the twelfth-grade program is still undecided and various proposals are under discussion.

A decade ago the pattern was fairly consistent: algebra in the ninth grade, plane geometry in the tenth grade, advanced algebra in the eleventh grade. The appropriate twelfth-grade offering is now acute in small as well as large high schools because of the quickening pace of curriculum development in mathematics. The improved materials and the shift of emphasis in grades seven and eight have produced some students who enter grade nine having a background of algebra. Thus, many schools are finding it necessary to provide something different from existing courses for these accelerated and enriched groups of students when they reach the twelfth grade. The trend toward elimination of solid geometry as a separate course through fusion with plane geometry, even with no other changes, creates an open semester in grade twelve.[1]

The Commission on Mathematics of the College Entrance Examination Board in 1959 gave three different proposals for twelfth-grade mathematics, including strong endorsement of the inclusion of some probability theory.[2] The School Mathematics Study Group has proposed matrix algebra and elementary functions.[3] Calculus has been extensively discussed as a possible subject for high school seniors. A course in computer mathematics is also gaining adherents as computers become increasingly important in our society. Thus, a current problem in high school mathematics education concerns the question of what mathematics topics ought to be taught to twelfth-grade mathematics students.

One of the most recent and complete studies of the emerging twelfth-grade mathematics program was a U. S. Office of Education survey conducted by Woodby. Information was obtained from 66 high schools in 20 states by means of correspondence, classroom visits, and interviews with teachers and administrators. Woodby found that calculus with analytic geometry was the course most frequently offered to those students who were able to take a fifth course in mathematics at the high school level. However, it was recommended that courses in calculus of less than a full year in duration not be offered.[4] This is in accord with the CEEB Commission on Mathematics in 1959.[5]

McKillip found that the grades of students who had at least one semester but less than two complete semesters of calculus in high school were not significantly different from the grades they would have been expected to earn without high school calculus. The students who had two semesters of calculus in high school made significantly better than the grades they would have been expected to earn.[6]

Some mathematicians take a dim view of offering calculus in high school, while others believe that capable students can and should study calculus before entering college. Different points of view exist which have been emphatically expressed at professional meetings and in the literature. Blank[7], Ferguson[8], and other writers supporting calculus in high school, generally agree that students should have completed the prerequisite courses by the end of the junior year and that the teacher should be fully qualified to teach a college level course in calculus.

Allendoerfer expressed the case against calculus when he wrote:

> Calculus is frequently taught at the wrong time, by the wrong people, and in the wrong way. It is high time we gave this matter our urgent attention. . . . The pressures on school systems to modernize their mathematics teaching are all to the good; however, the superintendent has tried to get off the hook by offering half-baked calculus to unprepared students in classes with incompetent teachers.[9]

Allendoerfer argues that no school should attempt to teach any calculus, probability, matrix algebra, or finite mathematics until analytic geometry has been properly presented to the students.

In the spring of 1964, Buchanan sent a questionnaire to the chairman of each of the 223 departments of mathematics of the colleges and universities located in the United States which offered a graduate program. He found that 61 per cent were opposed to both a unit on calculus in any form and a semester course in calculus. If the first semester of the twelfth grade is devoted to elementary functions, then the survey indicated that the preferred course for the second semester was analytic geometry, additional elementary functions, probability and statistics, or matrix algebra, in that order.[10]

In the article previously mentioned, Woodby found that there are many different courses being taught and still others are in the planning stage. There is no particular program that seems to be the most appropriate at the present time. He notes that most of the advanced courses are either calculus and analytic geometry or algebra and analysis intended to prepare students for calculus. He concludes that many high schools are teaching calculus courses of good quality; however, there is a trend toward the teaching of nonrigorous courses in calculus that emphasize only the mechanics of differentiation and integration.[11]

Grossman asserts that for some college-bound students who are ready for the calculus and who are mature enough to accelerate, a calculus course may be satisfactory. He raises the question of why we want to accelerate so many. He thinks that a more worthwhile objective would be enrichment rather than acceleration. Grossman points out that many courses in calculus are "once over lightly" approaches with a minimum of rigor and understanding. He argues that by postponing the study of calculus for one year, with the added maturity and added enrichment that the twelfth grade can provide, the student's understanding of the concepts of the calculus will more than repay the wait.[12]

Woodby recommends that experimentation with various twelfth-grade courses should continue. He recommends that seminar-type courses should be developed and that the colleges and universities should provide guidance in the development of twelfth-grade programs. He also notes that the trend is toward the offering of calculus.[13]

In addition to suggesting the need for enrichment, many writers have specified particular enrichment topics. For example, Grossman recommends the following topics as areas of enrichment for a twelfth-grade program: nature of number systems, isomorphic systems, linear algebra, abstract systems (groups, rings, and fields), Boolean Algebra, probability, elementary functions, and computer mathematics.[14]

Hollingstead suggested that many topics from number theory are appropriate for high school seniors.[15] In his famous essay, "A Mathematician's Apology," Hardy noted the importance of number theory when he wrote:

> The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes or reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and at least ten times as entertaining as the same amount of Calculus for Engineers.[16]

Filipponi suggested that topics such as the fundamental theorem of arithmetic, prime numbers, the set of real numbers, groups, theory of sets, and elementary topology would be appropriate for high school seniors.[17] The Oklahoma State Committee on the Improvement of Mathematics Instruction indicated that such topics as convex sets, Boolean Algebra, probability models, inequalities, group theory, conic sections, finite and infinite series, finite mathematical systems, computer science, mathematical induction, and topology are appropriate for enrichment for talented students in grades ten through twelve.[18]

A consideration of the suggested enrichment topics in light of Woodby's proposed seminar type course or independent study programs involving enrichment leads the writer to the following problem.

Statement of the Problem

The purpose of this study is to develop enrichment topics in mathematics for twelfth-grade mathematics students. The materials developed are designed for senior mathematics students who have completed a minimum of basic algebra, geometry, and advanced algebra.

Scope of the Study

The topics developed in this study were carefully selected from the topics suggested in the literature. Topics were selected from the fields of number theory, abstract algebra, topology, geometry, and probability theory. Topics from these fields were chosen to give the students a broader perspective of the domain of mathematics and to reinforce many of the fundamental concepts of mathematics such as sets, relations, functions, isomorphism, and so on. The approach used for each topic varies somewhat with the sophistication of the concepts involved. The approach to groups and graph theory is rather intuitive, while the approach to Farey fractions, fields, finite geometries, and probability theory is more rigorous.

The importance of the axiomatic method was stressed in the development of algebraic and geometric systems. The proofs to most of the theorems are given, although the teacher might not actually expect the students to be able to supply the proof to a given theorem since a considerable amount of originality and insight into the problem is required. The proofs, however, are structured in terms of concepts that should be familiar to the students, and the students should be able to understand the proofs.

In addition to the basic manipulative skills of algebra and the basic concepts of geometry, the presentation of topics assumes that the students are familiar with the basic properties of the real number system. The student should also be somewhat familiar with proof by mathematical induction and indirect proof. Moreover, the students should have been exposed to the basic rudiments of set theory.

If a concept arises that might be somewhat unfamiliar, a reference is given so that additional information can be obtained if the concept is not clear. Appendix A provides a ready source of collateral references on the various topics covered so that students or teachers can find additional information on a specific topic. References are also given on related topics so that if a student or group of students become interested in some area the teacher could suggest other topics of a similar nature for study.

Significance of the Study

The primary contribution of this dissertation is the development of reference materials for enrichment topics for high school senior mathematics students. The materials attempt to incorporate many of the topics suggested in the literature. The treatment of these topics is original in many cases. The materials developed in this study are quite flexible. They could be used to supplement any of the various suggested twelfth-grade courses such as elementary functions, analytic geometry, and so forth. The materials could be used as seminar topics in a mathematics laboratory or a Math 12X course offered in many high schools as an additional elective in the twelfth grade (i.e., in place of calculus or concurrent with calculus). Although the primary intent of the materials is enrichment for twelfth-grade mathematics students, many of the topics could be used for enrichment for grades nine through twelve for talented students.

The materials could also be used very appropriately as independent study topics to augment most any type of high school mathematics curriculum. The materials are developed in such a manner that any portion or section could be presented separately.

Summary and Overview

In this chapter the writer has developed the background for the problem, stated the problem, explained the scope of the study, and indicated the significance of the study.

Chapter II is a development of a topic from the field of number theory which has its derivation in the observations of a geologist named John Farey in 1816. The idea of Farey fractions is developed in a rather heuristic manner initially appealing to the intuition of the students' knowledge of common fractions. After certain basic conjectures about Farey fractions have been established, this theory is then used to give a rational approximation of an irrational number.

Chapter III is an intuitive introduction to finite groups. The approach is concrete in nature. Interesting topics such as loops and braids are also introduced. Several games such as the network game and tangliods are illustrated as amusing applications to the theory of groups. Chapter IV is an extension of the theory of groups. The field under consideration is an extension of the integers, that is, a field is developed as ordered triples of integers. Various properties of fields are considered through the study of this one algebraic system.

Chapter V is a discussion of various Euclidean and non-Euclidean finite geometries. The importance of the undefined terms "point" and "line" are emphasized and the essential properties of independence, consistency, and completeness of postulates are considered. Theorems are proven in each of the different geometries.

Chapter VI is a consideration of some of the interesting applications of graph theory. Initially, the famous Königsberg Bridge Problem is considered as motivation for the study of graphs. Gradually, the intuitive notation of a graph is defined more abstractly in terms of a binary relation defined on a set. Some of the fundamental theorems of graph theory are proven and solutions are given to some of the historically famous problems such as Hamilton's Travelers Dodecahedron problem.

Chapter VII is a set theoretic approach to finite probability. The basic notations of probability are developed from a set of three basic axioms. Various examples are given to illustrate the applications of the theory that is developed.

Chapter VIII includes a summary and recommendations for further study.

FOOTNOTES

[1] L. G. Woodby, *Emerging Twelfth-Grade Mathematics Programs* (Washington, 1965), p. 1.

[2] Commission on Mathematics of the College Entrance Examination Board. *Report of the Commission on Mathematics: Program for College Preparatory* (New York, 1959), p. 12.

[3] School Mathematics Study Group, *Mathematics for High School* (New Haven, 1962), p. 19.

[4] Woodby, pp. 1-40.

[5] Commission on Mathematics of the College Entrance Examination Board, p. 14.

[6] W. D. McKillip, "The Effects of High School Calculus on Students' First Semester Calculus Grades at the University of Virginia," *The Mathematics Teacher*, LIX (May, 1966), pp. 470-472.

[7] A. A. Blank, "Remarks on the Teaching of Calculus in the Secondary School," *The Mathematics Teacher*, LII (November, 1960), pp. 537-539.

[8] W. E. Ferguson, "Calculus in the High School," *The Mathematics Teacher*, LIII (October, 1960), pp. 451-453.

[9] C. B. Allendoerfer, "The Case Against Calculus," *The Mathematics Teacher*, LVI (November, 1963), p. 483.

[10] O. L. Buchanan, "Opinions of College Teachers of Mathematics Regarding Content of the Twelfth-Year Courses in Mathematics," *The Mathematics Teacher*, LVIII (March, 1965), pp. 223-225.

[11] Woodby, p. 35.

[12] George Grossman, "Advanced Placement Mathematics for Whom," *The Mathematics Teacher*, LV (November, 1962), pp. 560-566.

[13] Woodby, p. 36.

[14] Grossman, p. 562.

[15] Irving Hollingstead, "Number Theory--A Short Course for High School Seniors," *The Mathematics Teacher*, LX (March, 1967), pp. 222-227.

[16] G. H. Hardy, "A Mathematician's Apology," The World of Mathematics, ed. J. R. Neuman (New York, 1956), p. 2032.

[17] S. R. Filippone, "A Course of Basic Mathematical Concepts for Advanced High School Students," The Mathematics Teacher, LIII (April, 1960), pp. 256-259.

[18] J. H. Zant, Improvement of Mathematics Instruction in Oklahoma Grades K-12 (Oklahoma City, 1967), pp. 39-40.

CHAPTER II

FAREY FRACTIONS

The study of common fractions has long intrigued man. Beginning with the rules of calculation and properties of the integers, it would appear that there is nothing so mysterious about a common fraction a/b where a and b are integers and where $b > 0$. Definition 2.1 exhibits a condition for equivalence of two common fractions, while Definition 2.2 presents an inequality which insures an ordering of the common fractions.

Definition 2.1. $a/b = c/d$ iff $ad = bc$.

Definition 2.2. $a/b < c/d$ iff $ad < bc$.

If we stipulate that $a/b < c/d$ means the same as $c/d > a/b$, then it is obvious that the trichotomy property holds for common fractions; that is, for any two fractions x/y and z/w one and only one of the following is true: $x/y < z/w$, $x/y = z/w$, or $x/y > z/w$. However, there are infinitely many fractions which are equivalent to a given fraction. For example, $12/18 = 14/21 = 10/15 = 2/3 = \ldots$. This concept of a class of fractions each equivalent to a given fraction was a point of concern for the early mathematician. It is normally taken for granted that among the infinitely many fractions which are equivalent there is exactly one which is in reduced form with the numerator and denominator having no common divisor except 1.

A geologist named John Farey in 1816 made a very interesting observation about a certain set of reduced fractions between 0 and 1. He wrote down a sequence of reduced fractions between 0 and 1 whose denominators were limited by a number n.[1]

Listed in Figure 1 below are the first six rows of Farey's fractions.

n = 1: 0/1, 1/1

n = 2: 0/1 1/2, 1/1

n = 3: 0/1, 1/3, 1/2, 2/3, 1/1

n = 4: 0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1

n = 5: 0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 1/1

n = 6: 0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1

Figure 1

At first glance, these fractions may not appear to be very interesting or profound; however, it turns out that Farey's observation was quite remarkable. These fractions have some very unusual properties.

After a thorough investigation of the fractions in Figure 1, a student should be able to detect most of the following relationships.

1. Each fraction appears in reduced form.

2. Each fraction a/b satisfies $0 \leq a/b \leq 1$.

3. The denominator of each fraction in a given row is less than or equal to the number of the row.

4. In each row, the fractions are linearly ordered by "<".

5. Once a fraction appears in a row it appears in each subsequent row.

6. No two consecutive fractions have the same denominator except in the first row.

7. For any two consecutive fractions a/b, c/d in the nth row, $ad - bc = -1$.

It should be noted that these relationships are only conjectures based on observations of the first six rows. These conjectures may or may not be true for an arbitrary n. Before the validity of these conjectures can be tested, one needs to discover some general method for constructing a table of Farey fractions with n rows. First, rearrange the fractions in Figure 1 in a slightly different manner.

row 1	0/1												1/1
row 2	0/1						1/2						1/1
row 3	0/1				1/3		1/2		2/3				1/1
row 4	0/1			1/4	1/3		1/2		2/3	3/4			1/1
row 5	0/1		1/5	1/4	1/3	2/5	1/2	3/5	2/3	3/4	4/5		1/1
row 6	0/1	1/6	1/5	1/4	1/3	2/5	1/2	3/5	2/3	3/4	4/5	5/6	1/1

Figure 2

Analyzing rows 1 and 2, 1/2 is the only fraction inserted. Analyzing rows 2 and 3, 1/3 and 2/3 were inserted. What is the relationship between 0/1, 1/2, 1/1; 0/1, 1/3, 1/2; and 1/2, 2/3, 1/1? One noticeable relationship is the following: $1/2 = (0 + 1)/(1 + 1)$, $1/3 = (0 + 1)/(1 + 2)$, and $2/3 = (1 + 1)/(2 + 1)$.

<u>Conjecture 2.1</u>. If a/b, a'/b', and a''/b'' are three consecutive Farey fractions in the nth row, then $a'/b' = (a + a'')/(b + b'')$.

Is this conjecture true for the sixth row of the table in Figure 2? Even if the conjecture is true for any n, will this relationship allow one to systematically generate a table of n rows? To answer this question, note that the fractions appearing in the nth row that did not appear in the (n - 1)st row will have denominator n. Thus if a/b, a'/b' are consecutive fractions in the (n - 1)st row and $b + b' = n$, then $(a + a')/(b + b')$ appears in the nth row (assuming the above conjecture is true!). This approach may lead to a method of generating the nth row from the (n - 1)st row which, in general, will yield a systematic method of constructing a table of n rows. Before attempting to prove the above conjecture, it is necessary to prove a result that was conjectured by Farey and later proven by the famous mathematician, A. L. Cauchy.[2]

<u>Theorem 2.1</u>. For any two consecutive Farey fractions a/b, c/d in the nth row, $ad - bc = -1$. Note that $ad - bc = -1$ is equivalent to

$$\begin{vmatrix} a & c \\ b & d \end{vmatrix} = -1.$$

Proof: The proof of this theorem is by mathematical induction. The statement is certainly true for n = 1, 2, 3, 4, 5, 6 by inspection. Thus assume it to be true for n and then show that it is true for n + 1. Let a/b be a reduced fraction not in the nth row and then $b > n$.

Thus, $0 < a/b < 1$ and a/b is between some two consecutive Farey fractions h/k and t/m in the nth row by the definition of Farey fractions. If $\alpha = \begin{vmatrix} a & h \\ b & k \end{vmatrix}$ and $\beta = \begin{vmatrix} t & a \\ m & b \end{vmatrix}$, then $\alpha = ak - bh$ and $\beta = tb - am$. Since $h/k < a/b < t/m$, then $\alpha \geq 0$ and $\beta \geq 0$. Consider the system of equations: $\begin{array}{l} ak - bh = \alpha \\ \underline{-am + bt = \beta} \end{array}$. Solving these equations for a and b, yields:

$$a = \frac{\begin{vmatrix} \alpha & -h \\ \beta & t \end{vmatrix}}{\begin{vmatrix} k & -h \\ -m & t \end{vmatrix}} = \beta h + \alpha t \quad \text{and} \quad b = \frac{\begin{vmatrix} k & \alpha \\ -m & \beta \end{vmatrix}}{\begin{vmatrix} k & -h \\ -m & t \end{vmatrix}} = \beta k + \alpha m.$$

Therefore, $h/k < (\beta h + \alpha t)/\ (\beta k + \alpha m) < t/m$. If $\alpha = 0$, then $a/b = \beta h/\beta k$ which is a reduced fraction only when $\beta = 1$. However, if $\beta = 1$, the $a = h$ and $b = k$ which implies that $b < n$. This contradicts the assumption that a/b is not in the nth row, therefore, $\alpha \neq 0$. A similar argument shows that $\beta \neq 0$. Hence, $a/b = (\beta h + \alpha t)/(\beta k + \alpha m)$, $\alpha \geq 1$, $\beta \geq 1$. Next, note that the smallest value for b occurs when $\alpha = 1$ and $\beta = 1$. Therefore, $a = h + t$ and $b = k + m$. But, $k + m = n + 1$ since a/b is in reduced form and b is as small as possible. Hence, $a/b = (h + t)/(k + m)$ and a/b satisfied Farey's theorem since

$$\begin{vmatrix} h & a \\ k & b \end{vmatrix} = \begin{vmatrix} h & (h+t) \\ k & (k+m) \end{vmatrix} = \begin{vmatrix} h & t \\ k & m \end{vmatrix} = -1 \text{ and}$$

$$\begin{vmatrix} a & t \\ b & m \end{vmatrix} = \begin{vmatrix} (h+t) & t \\ (k+m) & m \end{vmatrix} = \begin{vmatrix} h & t \\ k & m \end{vmatrix} = -1.$$ Thus, Farey's theorem holds for $n + 1$ and the theorem is true for all n by mathematical induction.

Definition 2.3. If h/k, z/w are any two consecutive Farey fractions in the nth row, then $(h + z)/\ (k + w)$ is called the mediant between h/k and z/w.

Theorem 2.2. The fractions which belong to the (n + 1)st row are mediants of the fractions in the nth row.

This theorem is a result of the proof of Theorem 2.1 and gives a method to systematically construct a table of Farey fractions with n rows. Note that this is the result earlier conjectured. Formally stated, the method for constructing a table of Farey fractions is given by the following. In the first row write 0/1 and 1/1. For n = 2, 3, 4, ... , use the rule: form the nth row by copying the (n - 1)st row in order, but insert the fraction (a + a')/(b + b') between the consecutive fractions a/b and a'/b' of the (n - 1)st row if (b + b') $\leq$ n. It is now possible to investigate some of the conjectures made earlier.

Definition 2.4. If a and b are integers with a $\neq$ 0 and there exists an integer c such that b = ac, then a divides b and is denoted by $a|b$.

Theorem 2.3. If $a|b$ and $a|c$, then $a|(bx + cy)$ for any x and y.

Proof: If $a|b$ and $a|c$, then there exist integers r and s such that ar = b and as = c. Then, bx + cy = arx + asy = a(rx + sy) so that $a|(bx + cy)$ for any x and y.

Theorem 2.4. Every fraction a/b in the table is in reduced form, that is, (a,b) = 1 (the greatest common divisor of a and b is 1).

Proof: Suppose that a/b, z/w are consecutive fractions in the nth row and that (z,w) = d, d $\neq$ 1. Then Theorem 2.1 implies that $\begin{vmatrix} a & z \\ b & w \end{vmatrix}$ = -1 or bz - aw = 1. Since $d|w$ and $d|z$, the $d|(bz - aw)$ by Theorem 2.3 which implies that $d|1$. But since d $\neq$ 1, this is a contraction.

Hence, the theorem is true.

Theorem 2.5. If $n > 1$, then no two successive fractions a/b, a'/b' in the nth row have the same denominator.

Proof: This theorem is proven indirectly. Suppose the a/b and a'/b' are consecutive fractions in the nth row and $b > 1$. If $a/b < a'/b'$, then $a + 1 < a' < b$. But then $a/b < a/(a - 1) < (a + 1)/ b \leq a'/b$ which implies that $a/(b -1)$ is between a/b and a'/b which is a contradiction. Therefore, no two successive fractions in the nth row have the same denominator.

Theorem 2.6. The fractions in each row are listed in order of their size; that is, if a_1/b_1, a_2/b_2, ..., $a_k/b_,$ are fractions in the nth row, then $a_i/b_i < a_{i+1}/b_{i+1}$ for $i = 1, 2, 3, \ldots, k$.

Proof: Suppose that a_i/b_i , a_{i+1}/b_{i+1} are consecutive fractions with $a_i/b_i > a_{i+1}/b_{i+1}$. Theorem 2.1 implies that $\begin{vmatrix} a_{i+1} & a_i \\ b_{i+1} & b_i \end{vmatrix} = -1$ or that $a_{i+1} b_i - a_i b_{i+1} = -1$. But $a_i/b_i > a_{i+1}/b_{i+1}$ implies that $b_{i+1}a_i > b_i a_{i+1}$ or that $b_i a_{i+1} - b_{i+1} a_i > 0$ which is a contradiction. Therefore, $a_i/b_i < a_{i+1}/b_{i+1}$ and the fractions are listed in order of their size.

The next theorem is adapted from a theorem given by Niven and Zuckerman.[3]

Theorem 2.7. If a/b and a'/b' are consecutive fractions in any row, then among all rational fractions with values between these two,

$(a + a')/(b + b')$ is the unique fraction with the smallest denominator.

Proof: The fraction $(a + a')/(b + b')$ will first appear in the $(b + b')$th row. Let x/y be any fraction between a/b and a'/b'. Now, $a'/b' - a/b = (a'/b' - x/y) - (x/y - a/b) = (a'y - b'x)/b'y + (bx - ay)/by \geq 1/b'y + 1/by = (b + b')/bb'y$. Therefore, $a'/b' - a/b = (a'b - b'a)/bb' = 1/bb' \geq (b + b')/bb'y$ which implies that $y \geq (b + b')$, then $(a'y - b'x)/b'y + (bx - ay)by = 1/b'y + 1/by$ which implies that $a'y - b'x = 1$ and $bx - ay = 1$. Solving these two equations for x and y yields $x = a + a'$ and $y = b + b'$. Therefore, $(a + a')/(b + b')$ is the unique fraction lying between a/b and a'/b'.

<u>Theorem 2.8</u>. If $0 \leq m \leq n$ and $(m,n) = 1$, then the fraction m/n appears in the nth and all later rows.

Proof: The proof of this theorem is by induction. It is certainly true for $n = 1$. Suppose that it is true for $n - 1$ and then show that it is true for n. Consider the fraction k/n where $(k,n) = 1$. The fraction k/n does not belong to the $(n - 1)$st row by the definition of Farey fractions. Thus, k/n must lie between two consecutive fractions a/b and a'/b' in the $(n - 1)$st row; that is, $a/b < k/n < a'/b'$. Also $a/b < (a + a')/(b + b') < a'/b'$ and $(a + a')/(b + b')$ does not belong to the $(n - 1)$st row which implies that $(b + b') > n - 1$ or that $(b + b') \geq n$. Theorem 2.7 implies that $n > (b + b')$. Hence, $n = b + b'$ which implies that $k = a + a'$. Thus, $k/n = (a + a')/(b + b')$ which belongs to the nth row and by mathematical induction it belongs to all later rows.

Note that a method has been developed to generate a given row from the previous row, but is it possible to find the fraction succeeding a given fraction in that row without generating the table? For example, is it possible to find a fraction x/y such that h/k and x/y are consecutive frations in the nth row? Using Theorem 2.1, it would follow that $kx - hy = 1$. Do there exist integers x_o, y_o so that $kx_o - hy_o = 1$? This is an important question. If there does not exist a solution to this equation, then there are no hopes of solving the problem at hand.

Definition 2.5. A Diophantine equation is an equation that has a solution in integers.

This type of equation is named after the Greek mathematician Diophantus of Alexandria who lived about 250 A. D.[4]

Theorem 2.9. If $(a,b) = 1$, then the Diophantine equation $ax + by = 1$ is solvable.

Proof: First, it is possible to assume without loss of generality that $o < a < b$. Since $(a,b) = 1$, a/b is a proper reduced fraction and consequently a/b is a Farey fraction. Consider the Farey fraction h/k where h/k, a/b are consecutive fractions in the nth row. If $h/k < a/b$, then Theorem 2.1 implies that $\begin{vmatrix} h & a \\ k & b \end{vmatrix} = -1$ or that $ak - bh = 1$. Therefore, $x = k$, $y = -k$ is a solution to the equation $ax + by = 1$.

Using Theorem 2.9, there does exist a solution to the equation $kx - hy = 1$. If (x_o, y_o) is a solution, then $x_o + rh$, $y_o + rh$ is also a solution. If $n - k < y_o + rk \leq n$, then there is a solution (x,y) of $kx - hy = 1$ such that $(x,y) = 1$ and $0 \leq n - k < y \leq n$. Note that $(x,y) = 1$ and $y \leq n$ requires that x/y be in the nth row and $x/y = h/k + 1/ky > h/k$. To see that this is true suppose that $x/y > h'/k'$ where h'/k'

is the next fraction following h/k. Then, $h/k < h'/k' < x/y$ and $x/y - h'/k' = (k'x - h'y)/k'y \geq 1/k'y$. But $h'/k' - h/k = (kh' - hk')/kk' \geq 1/kk'$. So, $1/ky = (kx - hy)/ky = x/y - h/k \geq 1/k'y + 1/kk' = (k + y)/kk'y$. But $(k + y)/kk'y > n/kk'y \geq 1/ky$ implies that $1/ky > 1/ky$. This is a contradiction and $x/y = h'/k'$ which implies that x/y is the next fraction following h/k.

Thus, there exists a method to find the succeeding fraction following a given fraction in the nth row. Suppose as an example one wanted to find the successor of 4/9 in the 13th row. First, find a solution (x_o, y_o) to the equation $9x - 4y = 1$. One solution is $x_o = 1$, $y_o = 2$. Then choose r so that $13 - 9 < 2 + 9r \leq 13$. Certainly $r = 1$ will make this inequality true. If $r = 1$, then $x = 1 + 4r = 5$ and $y = 2 + 9r = 11$. Thus, the required fraction is 5/11.

Definition 2.6. A Farey sequence of order n, denoted F_n, is the ascending sequence of all irreducible fractions between 0 and 1 whose denominators do not exceed n.

Therefore, $h/k \in F_n$ if $0 \leq h \leq k \leq n$, $(h,k) = 1$. Thus, F_1 is the first row of the table and F_n is the nth row of the table.

Theorem 2.10. If a_1, a_2, ..., a_k are the denominators of the fractions preceding from left to right in the Farey sequence of order n, then

$$\sum_{n=1}^{n-1} (a_j a_{j+1})^{-1} = 1.$$

Proof: The proof of this theorem is by mathematical induction. The statement is obviously true for $n = 1$. Assume the statement is true for $n = k$ and show that it is true for $n = k + 1$; that is, show that

$\sum_{j=1}^{k} (a_j a_{j+1})^{-1} = 1$ given that $\sum_{j=1}^{k-1} (a_j a_{j+1})^{-1} = 1$. First, note that the only difference in $\sum_{j=1}^{k} (a_j a_{j+1})^{-1}$ and $\sum_{j=1}^{k-1} (a_j a_{j+1})^{-1}$ occurs as a result of the insertion of new fractions in the nth row. For each h/k in the nth row that is not in the (n - 1)st row where $a/b < h/k < a'/b'$, note that $-1/bb' + 1/bb' + 1/kb' = (kb' + kb)/k^2bb' - 1/bb' = (k(b + b')/k^2(bb') - 1/bb' = [(b + b') - k]/kbb' = 0$ since $(b = b') = k$. Therefore, $\sum_{j=1}^{k-1} (a_j a_{j+1})^{-1} = \sum_{j=1}^{k} (a_j a_{j+1})^{-1}$ and the theorem is true for every n by induction.

Another interesting property of Farey sequences is due to a conjecture by Aaron.[5]

Theorem 2.11 (Aaron's Conjecture). The sum of the numerators of the fractions of a Farey sequence F_n is equal to one-half the sum of the denominators of the fractions of F_n.

Proof: The proof of this conjecture is given in the American Mathematical Monthly by Blade.[6] However, the following proof does not depend so heavily on the theory of numbers. Two lemmas are proven to facilitate the proof of this conjecture.

Lemma 2.11.1. If $h/k \in F_n$, then $(1 - h/k) = (k - h)/k$ and $(1 - h/n) \in F_n$.

Proof: If $h/k \in F_n$, then $0 \leq h/k \leq 1$. Therefore, $0 \leq (1 - h/k) \leq 1$. But $(1 - h/k) = (k - h)/k$ where $k \leq n$ which implies that $(k - h)/k \in F_n$ since $((k - h),k) = 1$. Hence $(1 - h/k) \in F_n$.

Lemma 2.11.2. If $h/k < 1/2$, then $(1 - h/k) > 1/2$.

Proof: $h/k < 1/2$ implies that $(h/k - 1) < (1/2 - 1)$ or $(1 - h/k > 1/2$. Aaron's conjecture can now be proven using these two lemmas. Let $A = \{h_i/k_i \mid h_i/k_i < 1/2 \text{ and } h_i/k_i \in F_n, \text{ for all } i = 1, 2, \ldots, n\}$. By Lemma 2.11.1, $(1 - h_i/k_i) > 1/2$ and $(k_i - h_i)/k_i \in F_n$ for $i = 1, 2, 3, \ldots, n$. Thus, taking the sum of the numerators of the fractions in F_n, $\sum_{i=1}^{n} h_i + \sum_{i=1}^{n} (k_i - h_i) + 1 = \sum_{i=1}^{n} k_i + 1$. Similarly, summing the denominators of the fractions in F_n, $\sum_{i=1}^{n} k_i + \sum_{i=1}^{n} k_i + 2$ $= 2 \sum_{i=1}^{n} k_i + 2$. Hence, the sum of the numerators divided by the sum of the denominators yields $(\sum_{k=1}^{n} k_i + 1) /(2 \sum_{i=1}^{n} k_i + 2) = 1/2$ and the conjecture is proven since n is arbitrary.

At this point in the discussion, all of the earlier conjectures have been proven. Although Farey fractions have a very simple beginning, it is possible to put the theory thus far developed to work to prove some rather useful results concerning rational approximations of irrational numbers. It is strange in a sense how a mathematician can begin with a very simple idea and keep enlarging its applications. This is one of the inherent beauties of mathematics.

Let μ be an irrational number. Suppose one wishes to find a rational approximation of μ.

Theorem 2.12. For an irrational number, μ, and a positive integer n there exists a fraction h/k with denominator $k \leq n$ such that

$|\mu - h/k| < 1/(n + 1)k$.

Proof: In the Farey sequence of order n, one can find two consecutive fractions a/b and c/d such that $a/b < \mu < c/d$. Let $\alpha = (a + c)/(b + d)$, then either $a/b < \mu < \alpha$ or $\alpha < \mu < c/d$. Since α does not belong to F_n, then either $0 < \mu - a/b < \alpha - a/b$ or $0 < c/d - \mu < c/d - \alpha$. But, $\alpha - a/b = (a + c)/(b + d) - a/b = (bc - ad)/b(b + d) \leq 1/(n + 1)b$ since $bc - ad = 1$ by Theorem 2.1. Similarly, $c/d - \alpha = c/d - (a + c)/(b + d) = (cd + cd - ad - dc)/d(b + d) = 1/d(b + d) \leq 1/(n + 1)d$. Therefore, $0 < \mu - a/b \leq 1/(n + 1)b$ or $0 < (c/d - \mu) \leq 1/(n + 1)d$ and in either case there exists a fraction such that $|\mu - h/k| < 1/(n + 1)k$.

Theorem 2.13. If μ is an irrational number, then there exists a fraction h/k such that $|\mu - h/k| < 1/2k^2$.

Proof: Suppose that in the Farey sequence of order n, $a/b < \mu < c/d$. Now show that either $\mu - a/b < 1/2b^2$ or $c/d - \mu < 1/2d^2$. The theorem will be proven indirectly. Therefore, assume that μ is irrational and $\mu - a/b \geq 1/2b^2$ and $c/d - \mu \geq 1/2d^2$. Then, $c/d - a/b \geq 1/2b^2 + 1/2d^2 = (b^2 + d^2)/ 2b^2d^2$. But, $c/d - a/b = (cb - ad)/db = 1/bd$ by Theorem 2.1. This implies that $0 \geq (b^2 + d^2)/2b^2d^2 - 1/bd =$

$(b^3d + bd^3 - 2b^2d^2)/ 2b^2d^2bd = (b - d)^2/ 2b^2d^2$. However, $0 \geq (b - d)^2/2b^2d^2$ is true only when $b = d$. But, $ad - bc = -1$ implies that $b = d = 1$. Hence, for a Farey sequence of order $n > 1$, $\mu - a/b \geq 1/2b^2$ and $c/d - \mu \geq 1/2d^2$ is false. So that there exists a fraction h/k such that $|\mu - h/k| < 1/2k^2$.

Now, is it possible to get a better approximation? That is, does there exist a fraction h/k such that $|\mu - h/k| < 1/ck^2$ where $c > 2$?

This question was answered completely by A. Hurwitz.[7] He proved the following theorem.

Theorem 2.14. Given any irrational number μ, there exists infinitely many different rational numbers h/k such that $|\mu - h/k| < 1/\sqrt{5}\,k^2$.

Hurwitz also proved that $\sqrt{5}$ is the best possible constant; that is if $\sqrt{5}$ is replaced by any larger value the above theorem is not true.

Strangely enough, the concept of Farey sequences can be related to geometry in a very special way.

Definition 2.7. A Ford circle, C(h/k), is a circle in the complex plane in the form $|z - (h/k + i/2k^2)| = 1/k^2$, where h/k is a Farey fraction.

A Ford circle C(h/k) has its center at $h/k + i/2k^2$ and has radius $1/2k^2$. C(h/k) lies in the upper half-plane and is tangent to the x axis at x = h/k.

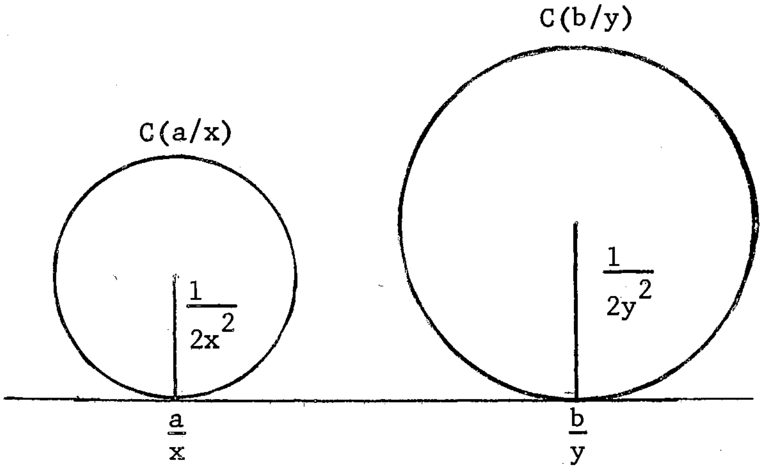


Figure 3

Ford circles have a very intriguing property which is stated in the following theorem.

Theorem 2.15. Two distinct Ford circles never intersect. They are tangent iff their fractions are adjacent in some Farey sequence.

Another configuration is peculiar to these Ford circles. If a/b, c/d, and e/f are three consecutive Farey fractions, then C(a/b), C(c/d), and C(e/f) are mutually tangent circles. Figure 4 illustrates this situation.

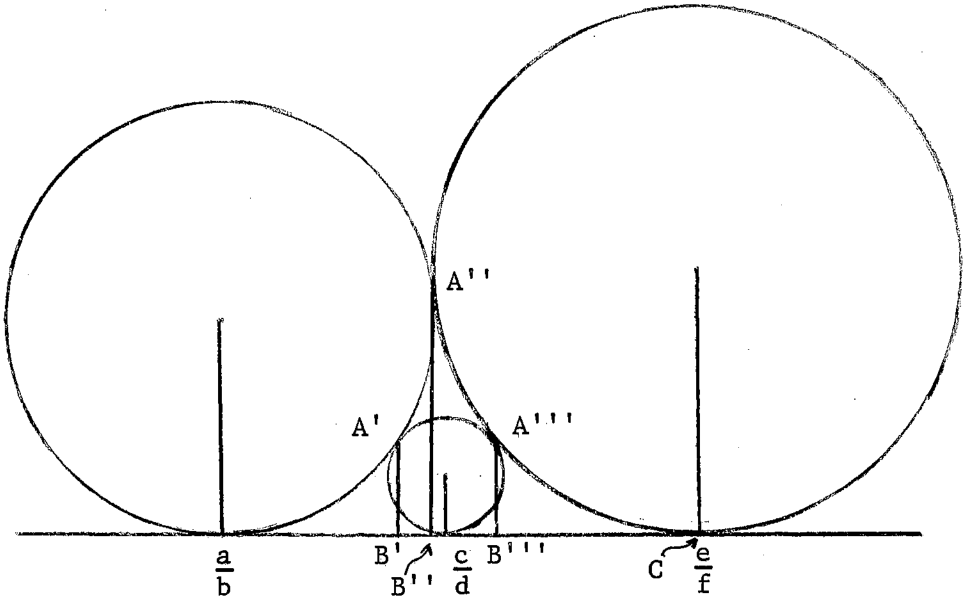


Figure 4

The above configuration forms some rather interesting figures. Geometric figures such as those illustrated by A''B''C and A'''B'''C are called circular triangles.

It turns out that this rather remote concept of Ford circles can be used to prove Theorem 2.14. The proof is given in Radamacker.[7]

Hopefully, presentation of this concept originated by Farey and the development of the related mathematical theory, shows some very important aspects of the developmental nature of mathematics. The fact that the rather simple concept of Farey fractions can be used to give a good rational approximation of an irrational number is remarkable.
The Appendix includes additional references pertaining to Farey fractions and other related topics such as Lucas and Fibonacci numbers.

FOOTNOTES

[1] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers (Oxford, 1938), p. 64.

[2] L. E. Dickinson, History of the Theory of Numbers (Washington, 1923), p. 43.

[3] Ivan Niven and Hubert S. Zuckerman, An Introduction of the Theory Numbers (New York, 1966), p. 142.

[4] Ibid., p. 103.

[5] J. A. Blade, "Some Characteristic Properties of the Farey Series," The American Mathematical Monthly, LXIII (1966), p. 50.

[6] Ibid., pp. 50-52.

[7] Hans Radmacher, Lectures on Elementary Number Theory (New York, 1964), p. 40.

CHAPTER III

GROUPS, LOOPS, AND BRAIDS

Frequently, secondary mathematics students have the notion that mathematics is strictly a quantitative science. The theory of groups is one of the important non-quantitative branches of mathematics. The concept of a group is relatively recent in the development of mathematics; however, the study of groups has been quite fruitful. Groups have become a powerful tool in the investigation of algebraic equations, geometric transformations, and problems in topology. Group theory is used today in many of the sciences; for example, physicists and chemists study the symmetries of particles and fields of force. In addition to being one of the most useful concepts in mathematics, groups are also one of the simplest.[1]

The study of groups has traditionally been delayed until rather late in a student's mathematical education. One reason that is often given for postponing the study of group theory is that a high degree of abstraction is inherent in group theoretical ideas, and the ability to cope with these abstract concepts comes only with mathematical maturity. However, Adler notes that it is often overlooked that group theory need not be approached in a highly abstract manner. A concrete approach to group theory can offer a basic understanding of the concepts involved and provide an excellent enrichment topic for high school students.[2]

The modern approach to secondary school mathematics emphasizes structure and the basic properties of the real system. Using this approach, the student should be familiar with the defining properties of major mathematical systems normally studied.

Definition 3.1. A mathematical system consists of three parts:

(1) A universal set

(2) Axioms or postulates which are statements assumed to be true with respect to the universal set

(3) Definitions yielding relations, operations, etc.

Definition 3.2. A binary operation on a set S is a rule which assigns to each ordered pair of elements of S a uniquely defined element of the same set S.

If S is a set of elements and # is a binary operation defined on the set S, the $< S, \# >$ is used to denote the mathematical system associated with S under the operation #.

Definition 3.3. A group is a mathematical system consisting of a binary operation, denoted here by #, defined on a non-empty set G that satisfies the following:

G.1 Closure For each $a,b \in G$, $a\#b \in G$

G.2 Associative For each $a,b,c \in G$, $(a\#b)\#c = a\#(b\#c)$

G.3 Identity There exist an element $e \in G$ such that for each $a \in G$, $a\#e = e\#a = a$.

G.4 Inverse For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}\#a = a\#a^{-1} = e$.

If one wants to test whether a given set of elements with a specific binary operation constitutes a group, one must check to see that each of the above axioms is satisfied. For example, consider the set of integers with the binary operation addition. Addition of integers is closed and associative. The identity element is 0 since for each integer a, $a + 0 = 0 + a = a$. If a is an integer, then -a is the inverse of a since $a + (-a) = (-a) + a = 0$. Therefore, the set of integers under addition forms a group. Since the set of integers is an infinite set, then it is referred to as an infinite group.

The set consisting of the numbers 1 and -1 with ordinary multiplication as the binary operation also forms a group. Closure and associative are obvious. The identity element is 1 and each element is its own inverse, that is, $(-1)^{-1} = -1$ and $1^{-1} = 1$. The number of elements in this group is finite and this is a finite group.

Many examples of groups arise quite naturally from mathematical systems that are studied in high school mathematics. Numerous examples of this type are given by Crouch and Beckman[3] and Laatsch[4].

A concrete approach to the study of finite groups is now considered. In general, if $< S, \# >$ is a mathematical system, then it would be nice if one had a systemic method for determining whether $< S, \# >$ is a group. One of the most common methods for analyzing finite groups was developed by Arther Caley.[5] Caley used a scheme similar to the familiar multiplication tables of arithmetic. He arranged the elements of the group in a square array, called a Caley square, so that the group elements are displayed in the top row and, in the same order, in the left column of the table. The entires in the table are determined by the group operation on the elements forming the row and column of that particular entry. For example, consider the Caley square for the set S = {1,-1} under ordinary multiplication given in Figure 5.

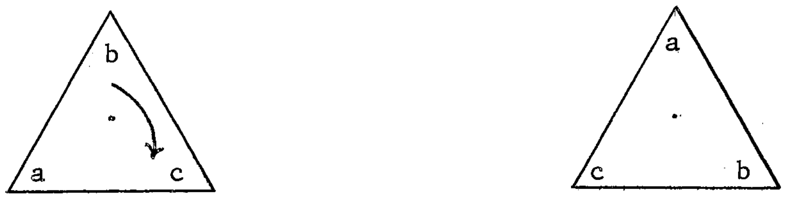
·	1	-1
1	1·1	1·-1
-1	-1·1	-1·-1

·	1	-1
1	1	-1
-1	-1	1

Figure 5

Notice that the Caley square allows one to check closure immediately, that is, every entry in the table is a member of the set under consideration. One also can determine the identity element by inspection. In this particular example, it is obvious that 1 is the identity element, since 1.a = a.1 = a for any non-zero integer a. In general, the identity element reveals itself in a Caley square since it is the element whose row is a copy of the column labels, column by column, and whose column is a copy of the row labels, row by row. Inverse elements can be discovered by observing in which row and column the identity element occurs, that is, 1·1 = 1 and -1·-1 = 1 so that each element is its own inverse. In general, associativity is the property that is most difficult to check. In this particular case, associativity is not so difficult to verify. The order of a finite group is the number of elements in the group.

The examples that have been considered thus far involve sets of numbers and familiar operations; however, the usefulness of the group concept is derived from its application to various sets of elements and operations. To illustrate this fact, consider a group whose elements are motions of an equilateral triangle. The motions will be considered as rotations in the plane of the triangle about an axis through its center. In order to establish a starting point, arbitrarily choose a particular position in the plane. For easy identification, assign a letter to each vertex. In Figure 6, the dot in the center represents the intersection of the axis of rotation and the plane. The second triangle shown in Figure 6 is a 120° clockwise rotation of the original triangle.



Initial Position

Position After 120° Clockwise Rotation

Figure 6

If the triangle is rotated 240° clockwise from the initial position, point a moves to the initial location of point c, b moves to the initial location of point a, and c moves to the initial location of point b. A rotation of 360° clockwise returns the triangle to its initial position. Similarly, one can rotate the triangle 120°, 240°, and 360° in a counterclockwise direction. It should be obvious that a counterclockwise rotation of 120° is equivalent to a clockwise rotation of 240°; that is, the triangle is in the same position. Thus, it is not too hard to visualize that several rotations may have the same net result. For example, a rotation of 480° clockwise is equivalent to 120° clockwise rotation.

In order to make this discussion more definite, consider the following two classes of rotations: S = {clockwise rotations of $120^{\circ} \pm (360k)^{\circ}$; k = 0, 1, 2, ...} and T = {counterclockwise rotations of $120^{\circ} \pm (360k)^{\circ}$; k = 0, 1, 2, ... }. The sets S and T define what is meant by a rotation of the triangle. Two rotations are the same or equivalent if they have the same effect.

Each of the rotations defined in S or T result in one of three basic positions. To best illustrate this fact, an equilateral triangle can be cut out of paper or cardboard and each vertex labeled as shown in Figure 6. It is much easier to visualize a rotation with a physical model present. In Figure 7, the three basic positions are illustrated and each rotation is labeled for future reference.

It may seem reasonable at this point to conjecture that the set of rotations defined in Figure 7 form a group. However, it should be noted that the definition of a group requires not only a set of elements but a binary operation defined on this set. Thus, define a binary operation # which means "followed by". That is, A#B means perform rotation A followed by rotation B. The rotation A#B is equivalent to the rotation I since the net result of A#B is I and is written A#B = I. Figure 8 illustrates the fact that A#B = I.

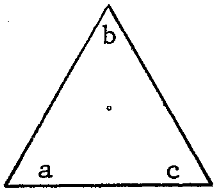
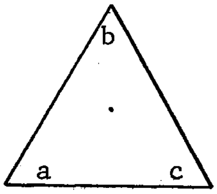
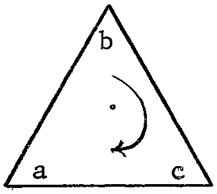
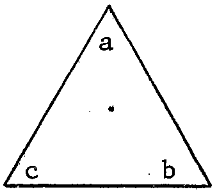
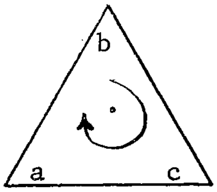
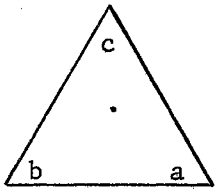
Notion	Symbol	Initial Position	Final Position
0^{o} rotation	I		
120^{o} clockwise rotation	A		
240^{o} clockwise rotation	B		

Figure 7

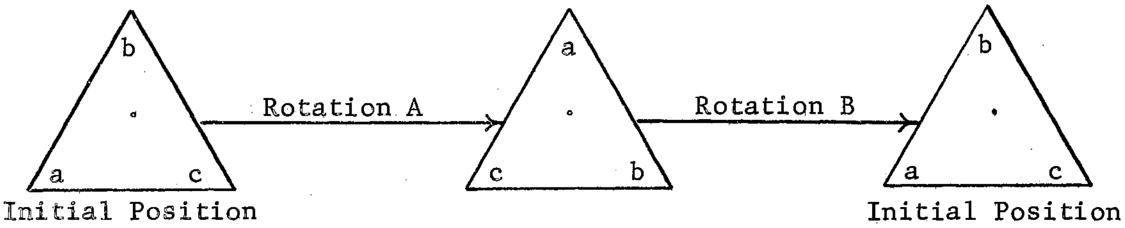


Figure 8

Using the physical model of the triangle, the remaining six products can be computed. As a matter of convention, one often refers to abstract operations as products even though the operations may not resemble multiplication in the normal sense. The group table or Caley square is often referred to as a multiplication table. The operation symbol is also often omitted, that is, A#B is written AB. The nine products associated with the three rotations of the triangle are given in the Caley square in Figure 9.

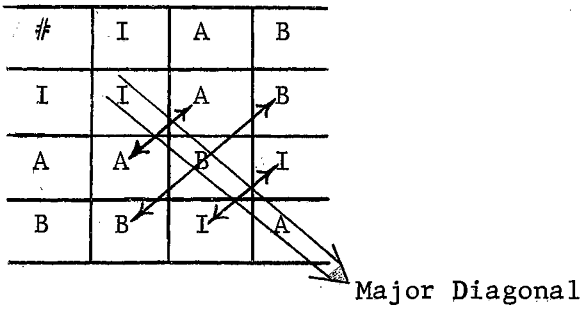
#	I	A	B
I	I	A	B
A	A	B	I
B	B	I	A

Figure 9

An examination of the products in the table in Figure 9 reveals that I is the identity element and that $A^{-1} = B$ and $B^{-1} = A$ since AB = BA = I. The table also shows that all elements commute with each other, that is, AB = BA, AI = IA, and BI = IB.

Definition 3.4. A group $< G * >$ is commutative iff for all elements $a, b \in G \quad a * b = b * a$. A commutative group is often called an abelian group.

An inspection of the symmetry about the major diagonal of a group table is the easiest method to check for commutativity. The major diagonal runs from the upper left-hand corner to the lower right-hand corner of the table. Figure 10 indicates the major diagonal and the symmetry of the respective products.



#	I	A	B
I	I	A	B
A	A	B	I
B	B	I	A

Figure 10

Thus, a finite group is commutative if and only if the multiplication table associated with the group has the property that products located symmetrically with respect to the major diagonal represent the same group element.

Associativity is the most difficult group property to verify. However, associativity should not be taken for granted since it is possible for a mathematical system to satisfy all of the group axioms except for associativity.

<u>Definition 3.5</u>. A mathematical system that satisfies group axioms G.1, G.3, and G.4 is called loop.

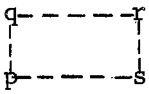
Let A = {e,a,b,c,d} and let the binary operation & be defined on A as indicated in Figure 11. It is not difficult to conclude that A is closed with respect to & and that e is the identity element. Furthermore, the table reveals that each element is its own inverse. Thus, < A, & > forms a loop. However, < A, & > does not form a group since the associative property does not hold. To see this, note that a&(b&c) = a&b = c and (a&b)&c = c&c = e. Therefore, a&(b&c) $\neq$ (a&b)&c.

&	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	b	e	b
c	c	c	b	e

Figure 11

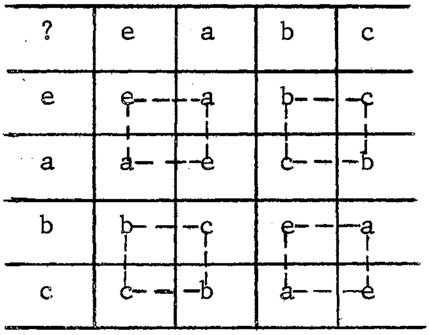
The fact that some systems form loops but not groups requires that a certain amount of care be given to associativity. Fortunately, there are methods by which associativity can be checked without having to test all possibilities. Checking all possibilities can become extremely cumbersome. In general, if a set has n elements, then there are n^3 different possibilities to check.

Zassenhaus developed a technique that reduces the number of computations considerably.[6] However, Watson gave a generalization of Zassenhaus' method which is substantially easier to employ. Watson's rule states:

> In the multiplication table of the loop choose any four places forming vertices of a rectangle. Suppose the entries are
>
> 
>
>
> If this loop is a group, then all other rectangles having p, q, and r as entries at successive vertices, with p and q sharing a column, will have s as the entry at the fourth vertex. The converse is also true.[7]

To illustrate Watson's method, consider the set S = {e,a,b,c} with the binary operation ? defined on S as indicated in the Caley square in

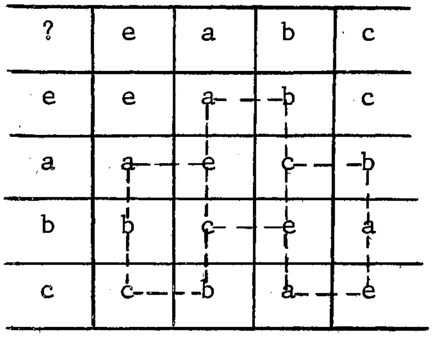
Figure 12. To illustrate Watson's method, the writer will not attempt to indicate all possible rectangles that would need to be checked; however, several different rectangular patterns will be illustrated. In Figure 12 below, the rectangle in the upper left of the table has a, e, and a at successive vertices, a and e in the same column, and e at the fourth vertex. The rectangle indicated in the lower right corner of the table is similar to the rectangle described above. Analogous observations can be made relative to the rectangles indicated in the upper right and lower left hand corners.



?	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Figure 12

The rectangles indicated in Figure 13 have c, a, and e as successive vertices with b as a fourth vertex while a and c are in the same column in each of the three rectangles. The procedure illustrated would be continued until all possibilities satisfying Watson's rule have been exhausted. If in each case the rule holds, then the loop is a group.



?	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Figure 13

One can simplify Watson's method somewhat by only considering the rectangles that have the identity element in one corner. For each of these rectangles, if the product of the entry that is in the same column as the identity element with the entry that is in the same row as the identity element is equal to the entry diagonally opposite the identity element, then the associative property is satisfied. For the lack of a better name, this will be referred to as the rectangle property. In other words, if e is the identity element and

$$\begin{tikzcd} e \arrow[r, dash] \arrow[d, dash] & x \arrow[d, dash] \\ y \arrow[r, dash] & z \end{tikzcd}$$

is a rectangle in some Caley square, then $yx = z$. To see that this condition is enough to guarantee that a loop is a group, consider a loop $< S, \cdot >$ which satisfies the rectangle property. If e is the identity element of S and r, s, and t are arbitrary elements of S, the $r^{-1} \in S$ and $rr^{-1} = e$. Now consider the rectangle indicated in Figure 14; and note that since the elements r, s, and t are arbitrary elements of S it is not necessary to fill in the table specifically.

$\cdot$	r^{-1}	t
r	e	rt
sr	s	$(sr)t$

Figure 14

Since s, r, t $\in$ S, then sr, rt, and (sr)t are elements of S by the closure property. The entry at the corner where r^{-1} row crosses the e column is r^{-1} since $r^{-1}e = r^{-1}$. The entry at the corner where the s row crosses the e column is s, since se = s. Likewise, the entry at the corner where the r^{-1} row crosses the r column is e and the entry at the corner where s crosses the r column is sr. Since the rectangle property is assumed, it follows that $(sr)r^{-1} = s$. Hence, the entries in the table in Figure 14 are justified and by the rectangle property, s(rt) = (sr)t. Since r, s, and t are arbitrary elements in S, then S must be associative with respect to the operation "." and $< S, \cdot >$ is a group. This restriction of Waston's method is probably the simplest method for checking associativity in tables for finite groups.

Using the groups of rotations of an equilateral triangle defined in Figure 7, add three additional motions and consider the resulting system. As in Figure 15, define three motions by flipping the triangle. The easiest way to think about this is as a rotation of 180^{o} about an altitude from one of the vertices.

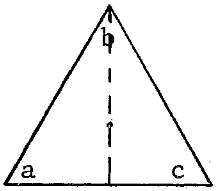
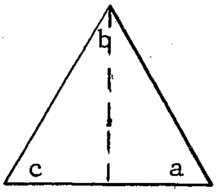
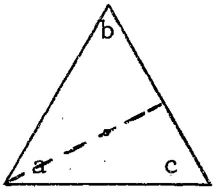
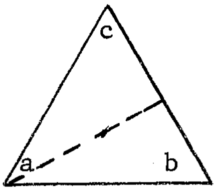
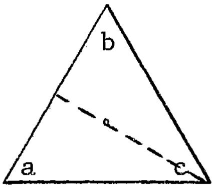
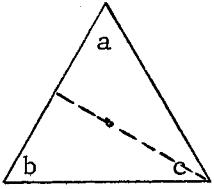
Motion	Symbol	Initial Position	Final Position
180^o rotation about the altitude from the top vertex	C		
180^o rotation about the altitude from the left vertex	D		
180^o rotation about the altitude from the right vertex	E		

Figure 15

Let S be the set of rotations I, A, B, C, D, and E defined in Figures 7 and 15. Let # be the binary operation "followed by" defined on S. Is < S, # > a group? An examination of the Caley square for < S, # > shown in Figure 16 reveals that < S, # > is a group of order 6.

< S, # > is often referred to as the group of symmetries of an equilateral triangle. It is suggested that the beginning student verify the above group table using a physical model. It is interesting to note that < S, # > is not a commutative group since C#D = A and D#C = B.

Another simple example of a group that involves rigid motions of a geometric figure is the rotations of a rectangle. This group is defined by the rotations illustrated in Figure 17.

#	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

Figure 16

Motion	Symbol	Initial Position	Final Position
No rotation	i	a b c d	a b c d
Rotate 180° clockwise	p	a b c d	d c b a
Rotate horizontally about the median	q	a b c d	c d a b
Rotate vertically about vertical median	r	a b c d	b a d c

Figure 17

If the binary operation "followed by" is defined on the set of rotations given in Figure 17, then one can form the group table given in Figure 18.

#	i	p	q	r
i	i	p	q	r
p	p	i	r	q
q	q	r	i	p
r	r	q	p	i

Figure 18

Since group multiplication is a generalization of ordinary multiplication, it seems reasonable to denote the group element A#A or AA as A^2 and AAA by A^3. Using this convention, the products in the group table in Figure 9 would be, AA = A^2 = B, AB = AAA = A^3 = I, BB = A^2A^2 = A^4 = A^3A = IA = A, BA = AAA = A^3 + i, and AI = IA = A. Thus, the table in Figure 9 could be written as in Figure 19.

It is interesting to note that every element of the group is a power of the single element A since I = A^3. A group with this property is said to be a cyclic group generated by the element A and A is called a generator.

#	I	A	A^2
I	I	A	A^2
A	A	A^2	I
A^2	A^2	I	A

Figure 19

<u>Definition 3.6</u>. A group G is cycle iff there is an element $a \in G$ such that for any $b \in G$ there is some integer k such that $b = a^k$.

Thus, the group of rotations of an equilateral triangle is a cycle group of order 3. Since A generates this group, one can write successive powers of A which exhibit a cyclic repetition of the basic pattern $A, A^2, A^3 = I$. This characteristic lends itself to a geometric interpretation. For example, if each element of the group represents a vertex of a triangle, then the group can be represented as a network of directed segments as shown in Figure 20 where each side of the triangle has a direction assigned to it as indicated by the arrow. Moving in the direction of the arrow corresponds to right multiplication, that is, moving from A^3 to A represents A^3A. Moving in the direction opposite the arrow corresponds to right multiplication by A^{-1}, the inverse of A. Hence, moving from A to I in the opposite direction of the arrow yields $A^{-1}A = I$. A network such as the one illustrated in Figure 20 is often called a Caley diagram or the graph of a group.

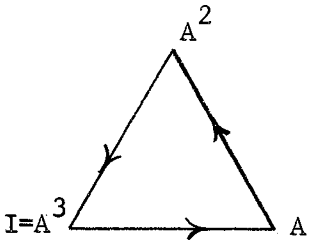


Figure 20

Definition 3.7. A Caley diagram is a network or graph that represents a group as a network of directed segments where the vertices correspond to elements and the segments correspond to multiplication by group generators and their inverses.

To further illustrate the idea of graphing a group consider the group defined in Figure 21. Is it possible to construct a Caley diagram for the group defined in Figure 21? To answer this question one must determine if the group is cyclic or find a generator for the group. If a is a generator, then a must generate the group, that is, successive powers of a will produce all the elements of the group.

#	i	a	b	c
i	i	a	b	c
a	a	b	c	i
b	b	c	i	a
c	c	i	a	b

Figure 21

Note that, $aa = b = a^2$, $ba = c = a^2a = a^3$, $ca = i = a^3a = a^4$, and $ia = a$. Thus, a is a generator. Notice that c is also a generator but b is not a generator. Using the fact that a generates the group, the group table can be written as follows:

#	i	a	a^2	a^3
i	a	a	a^2	a^3
a	a	a^2	a^3	i
a^2	a^2	a^3	i	a
a^3	a^3	i	a	a^2

Figure 22

The Caley diagram for the group defined in Figure 22 can now be constructed.

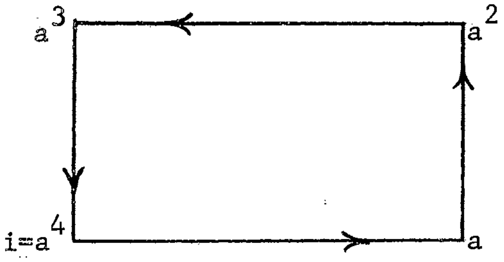


Figure 23

Modular arithmetic offers numerous examples of groups. Early in life a child is exposed to modular arithmetic when he first learns to tell time. In the ordinary clock arithmetic with 12 numbers, a strange type of addition was learned, that is, 9 + 4 = 1 and 6 + 8 = 2. These additions are thought of as rotations of the hands of the clock around the clock face.

This same idea can be extended to modular systems containing a different number of elements. Each number can be interpreted as a motion on the number line. For a specific example, consider a system, S_3, that contains the elements 0, 1, and 2. Think of these elements as representing three equally spaced points on a given circle, called units. This is illustrated in Figure 24.

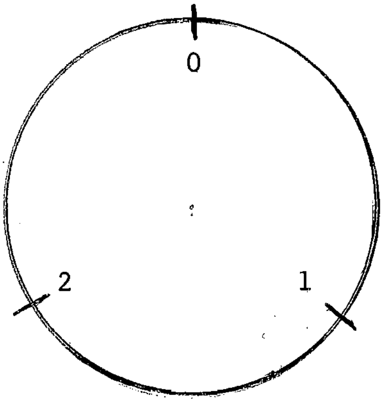


Figure 24

In order to define addition, denoted $\oplus$, interpret each number as a clockwise rotation of a whole number of units around the circle.

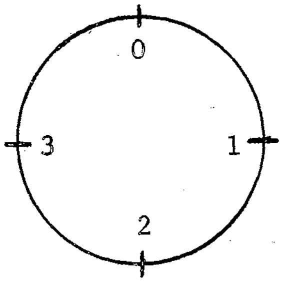
Thus, the number 0 represents a motion of zero units, 1 stands for a motion of 1 unit, and 2 stands for a motion of 2 units. Hence to find $2 \oplus 2$, start at 0 and move 2 units clockwise followed by a movement of 2 units clockwise which implies that $2 \oplus 2 = 1$. Similarly, $2 \oplus 3 = 2$. In Figure 25, a table is constructed to record the various sums for the set $S_3 = \{0,1,2\}$ under the binary operation +. Note that $< S_3, \oplus >$ forms a group.

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Figure 25

By a similar process, one can consider a modular system for $S_4 = \{0, 1, 2, 3\}$ and construct a physical model to illustrate the binary operation +. It is easy to verify that $< S_4, + >$ forms a group by checking the Caley square shown in Figure 26.

It is rather interesting to note that certain groups are very similar in an abstract sense. For example, consider the group of rotations of an equilateral triangle defined in Figure 8 and the group $< S_3, + >$ defined in Figure 25. In order to compare these groups, their group tables are shown in Figure 27.



$\oplus$	0	1	2	3
0	1	1	2	3
1	1	2	3	0
2	2	3	1	1
3	3	0	1	2

Figure 26

#	I	A	B
I	I	A	B
A	A	B	I
B	B	I	A

table a

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

table b

Figure 27

Note that the arrangement of symbols I, A, and B in table a is the same as the arrangement of the symbols 0, 1, and 2 in table b. Thus, whenever I appears in table a, 0 appears in table b; whenever A appears in table a, 1 appears in table b; and whenever B appears in table a, 2 appears in table b. Hence, if one starts with table a and interchanges the operation # and $\oplus$ and substitutes 0, 1, and 2 for I, A, and B, then table is obtained. Similarly, one could change table b to table a since these two tables only differ in the symbols that are used. Figure 28 illustrates the appropriate substitutions that change table b to table a.

$$\begin{tikzcd}
\oplus \arrow[r] & \# \\
0 \arrow[r] & I \\
1 \arrow[r] & A \\
2 \arrow[r] & B
\end{tikzcd}$$

Figure 28

If the tables for two groups are the same except for the differences in language or notation, then the groups are said to have the same structure and are called isomorphic groups. The concept of isomorphism is one of the fundamental concepts of mathematics.

To further illustrate the concept of isomorphism, consider the groups given in Figures 21 and 26. These group tables are reproduced in Figure 29 for easy comparison. It should be obvious that these two groups are isomorphic since the groups are related by the correspondence given in Figure 30.

Before leaving the topic of groups, one should investigate permutation groups which were the historical instigators of the study of groups. Emil Artin developed an interesting and unique approach to the study of certain types of permutation groups in his so-called "theory of braids".[58]

#	i	a	b	c
i	i	a	b	c
a	a	b	c	i
b	b	c	i	a
c	c	i	a	b

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figure 29

$\# \longrightarrow \oplus$

$i \longrightarrow 0$

$a \longrightarrow 1$

$b \longrightarrow 2$

$c \longrightarrow 3$

Figure 30

To illustrate Artin's approach, a simple example consisting of three strands is considered. Let S denote the set of configurations in Figure 31. Let "0" be the binary operation defined as follows:

<u>Definition 3.8</u>. If X and Y are any two members of S, then XOY designates the symbol which is formed by placing X and Y together so that the top points of Y coincide with the bottom points of X; and then mentally removing the coincident points and stretching the lines straight.

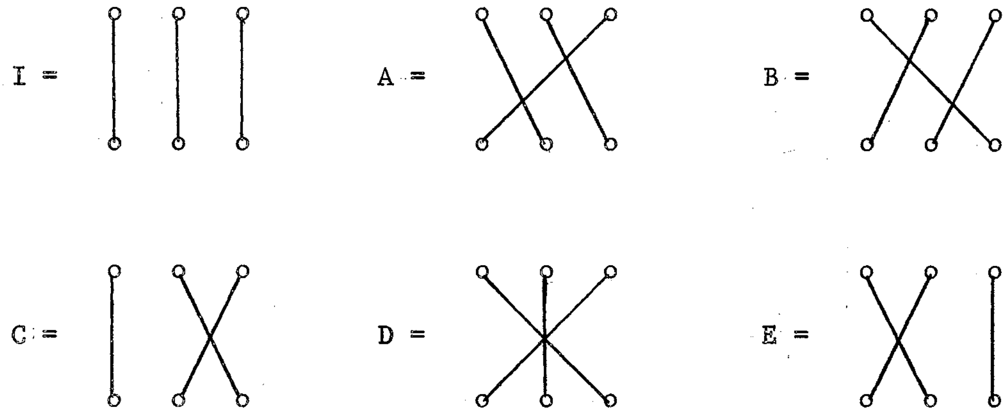
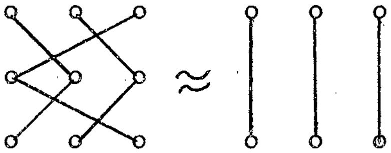


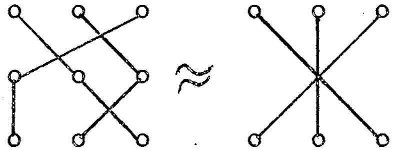
Figure 31

For example, AOB means



= I and

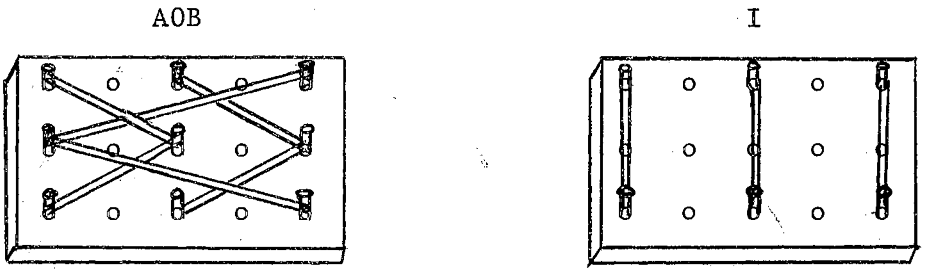
AOC $\approx$



= D.

Therefore, AOB = I and AOC = D. A physical model can be constructed to represent Artin's braids as defined above by using a pegboard or geoboard and rubber bands for strands. Figure 32 illustrates AOB.

Using a physical model or a mental model, the student should be able to construct the group table shown in Figure 33. The permutation group as defined in Figure 33 is the basis for a rather interesting game called a network tracing game. Since there are only three strands in the defining properties of this group, only three people can play. The game begins by drawing three vertical lines on a sheet of paper.



Initial Position

Position after removing the center pegs

Figure 32

O	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	D	E	C
B	B	I	A	E	C	D
C	C	E	D	I	B	A
D	D	C	E	A	I	B
E	E	D	C	B	A	I

Figure 33

One of the players holds the paper so that his friends cannot see what he is doing and randomly labels the lines A, B, and C where each player is associated with a letter. He then folds the top of the sheet of paper so that the letters are concealed. Figure 34 illustrates a possible play for the first player.

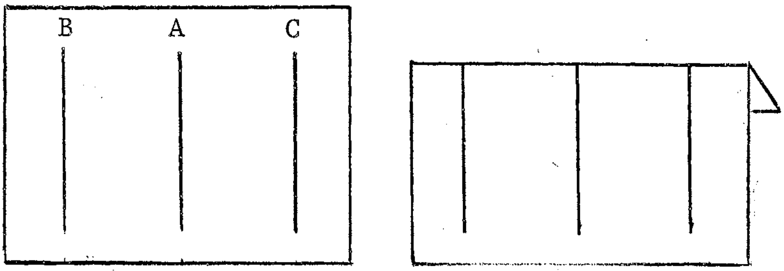
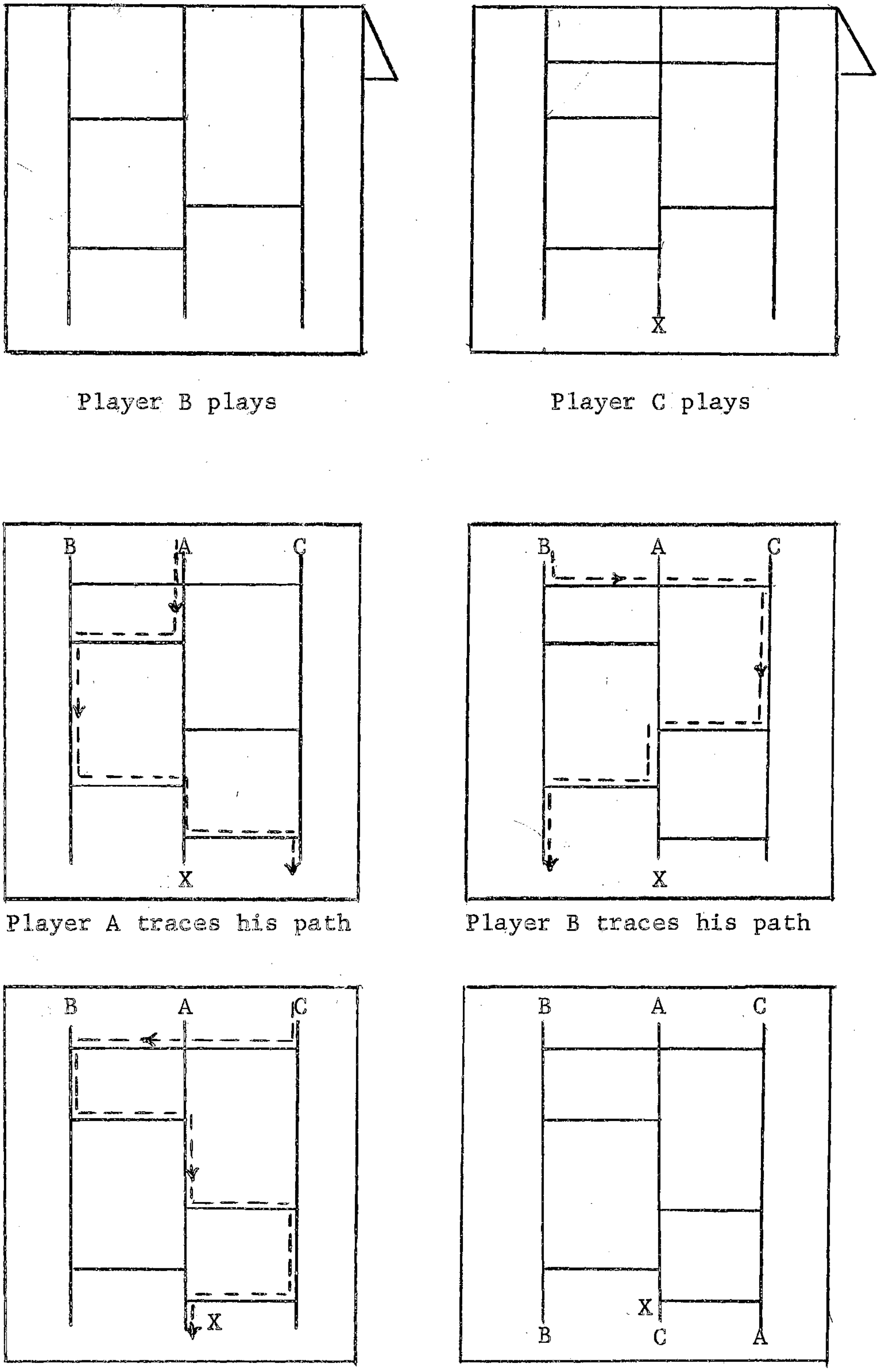


Figure 34

The second player is given the paper and he draws a series of random horizontal lines, called shuttles, each connecting two of the vertical lines. The third player adds a few more shuttles and then placês an X at the bottom of one of the vertical lines. The paper is then unfolded and player A starts at the top of column A and traces downward until he hits a shuttle. He then turns and proceeds to the end of the shuttle and turns downward again. This process is continued until player A reaches the bottom of a vertical line. Note that shuttles drawn from the first vertical line on the left to the last vertical line on the right cannot be entered from the center line. Player B and player C follow the same tracing process and the player that ends up at the X is the loser. Figure 35 gives a sample of the tracing process and shows each player's path assuming the shuttle pattern given in the upper left corner of the figure.

At first glance this network game may not appear to be related to the permutation group defined in Figure 33; however, a careful investigation would reveal that the configurations in Figure 36 represent the possible configurations involved in the network game.



Player B plays

Player C plays

Player A traces his path

Player B traces his path

Player C traces his path

Final Positions

Figure 35

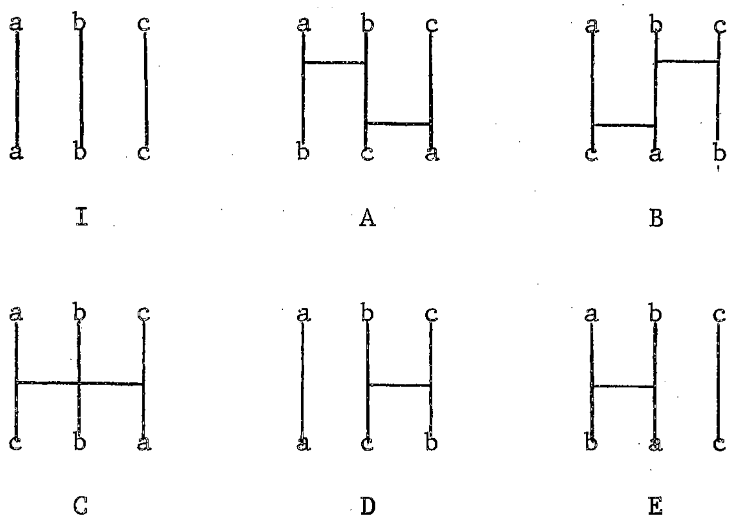


Figure 36

The configurations defined in Figure 36 produce the permutation group defined in Figure 33. The group table clarifies the above game. For example, shuttle pattern B followed by shuttle pattern C has the same effect as shuttle pattern E.

It is interesting to note that the network game will never permit two players to end their path on the same vertical line. This can be illustrated intuitively by just thinking of the three lines as three ropes, and each shuttle has the same effect on path order as crossing two ropes. It was this idea of visualizing this simple problem involving permutation groups in terms of ropes that lead Emil Artin to develop a rather elegant theory of braids.[9] In this theory, the elements of the group are weaving patterns and the operation consists, as in the network game, of following one pattern with another.

Piet Hein, a Danish mathematician, developed an unusual game called tangloids that involves braid theory.[10] To illustrate this game, first construct a physical model for easy reference. A triangular shaped piece of heavy cardboard or plywood and 3 pieces of cord or rope are all the materials that are needed. Three holes are punched in the flat end of the triangular plaque and the three cords are attached as shown in Figure 37. The cords should be fairly flexible and approximately two feet in length. It also helps if the cords are different colors, but it is not necessary. The other end of the three cords are attached to some stationary object such as a chair back.

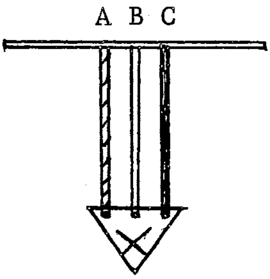


Figure 37

The plaque can be rotated in six different ways to form six different braids. It can be rotated sideways to the right or to the left; it can be rotated forward or backward between strands A and B; and it can be rotated forward or backward between strands B and C. Figure 38 shows the braid formed by a forward rotation between B and C. Is it possible to untangle this braid by weaving the plaque in and out through the strands, keeping the plaque horizontal, X-side up, and pointing forward at all times? The answer is no. However, if the plaque is given a rotation in any of the six different ways, the resulting braid can be untangled by weaving the plaque without rotating it.

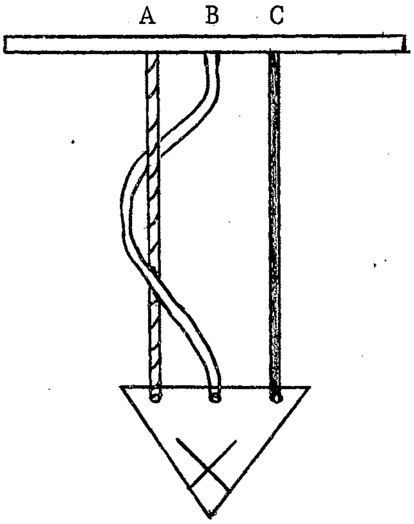


Figure 38

An interesting result of braid theory is the fact that all braids produced by an even number of rotations can always be untangled by weaving the plaque without rotating it; however, braids produced by an odd number of rotations can never be untangled. It makes a rather interesting game to let one player form a braid by rotating the plaque an even number of times. The second player then attempts to untangle the braid as quickly as possible. The player who untangles the braid the fastest is the winner. Some players even use a stop watch and keep tract of the score in seconds. For further explanation and examples of braid theory see Artin[11] and refer to the Appendix.

FOOTNOTES

[1] Irving Adler, Groups in the New Mathematics (New York, 1967), p. 7.

[2] Ibid., p. 8.

[3] Ralph Crouch and David Beckman, Algebraic Systems (Glenview, Illinois; 1966), pp. 32-65.

[4] Richard Laatsch, Basic Algebraic Systems: An Introduction to Abstract Algebra (New York, 1968), pp. 42-68.

[5] Israel Grossman and Wilhelm Manus, Groups and Their Graphs (New York, 1964), p. 14.

[6] Hans Zassenhaus, The Theory of Groups (New York, 1949), p. 4.

[7] Donald Watson, "Condition for a Loop to be a Group," The American Mathematical Monthly, LXXXIV, pp. 843-844.

[8] Emil Artin, "The Theory of Braids," Mathematics Teacher, LII (May, 1959), pp. 328-333.

[9] Ibid.

[10] Emil Artin, "Braids and Permutations," Annals of Mathematics, Second Series, XLVIII, 1947, pp. 643-649.

[11] Ibid.

CHAPTER IV

AN UNFAMILIAR FAMILIAR FIELD

The study of simple mathematical systems involving only one binary operation, such as groups, are quite interesting; however, most mathematical structures that high school students are acquainted with involve two major binary operations. The mathematical system involving two binary operations of principal importance is called a field. The concept of a field has been studied by mathematicians for many years; yet it can properly be considered a part of modern mathematics since much research is still being done in field theory.

Definition 4.1. A field is a mathematical system consisting of a set F and two binary operations which will be denoted by $\oplus$ and $\odot$ such that:

(1) F is a commutative group under $\oplus$.

(2) $F \cap \{i\}'$ is a commutative group under $\odot$, where i is the identity element with respect to $\oplus$.

(3) $\odot$ is distributive over $\oplus$, that is, for each $x, y, z \in F$ $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ and $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$.

Much of mathematics, and indeed much of the mathematics studied by a high school student deals directly or indirectly with numbers systems. Three very important number systems are examples of fields: the rational numbers, the real numbers, and the complex numbers.

The intent of this section is to present a slightly different mathematical system which is an extension of the integers. The system $< M, +, \cdot >$ is characterized by the following four definitions:

Definition 4.2. $(a,b,c) \in M$ iff a, b, c are integers and $c \neq 0$.

Definition 4.3. $(a,b,c) = (d,e,f)$ iff $(ac + b)f = (df + e)c$.

Definition 4.4. $(a,b,c) + (d,e,f) = (a + d, bf + ce, cf)$.

Definition 4.5. $(a,b,c) \cdot (d,e,f) = (ad, aec + dbf + be, cf)$.

An initial investigation of this system will reveal that the relation "=" given in Definition 4.3 is an equivalence relation. This equivalence relation induces a partition of the set M into mutually disjoint subsets called equivalence classes, that is, $(a,b,c) = \{ (x,y,z) \mid (ac + b)z = (xz + y)c \}$. Frequently, when dealing with equivalence classes it is not obvious that two elements belong to the same class. A process called reduction will, in many cases, help in this regard. For example, the elements $(7,9,51)$ and $(7,3,17)$ are in the same class and the reduction process can be generalized by showing that $(a,bn,cn) = (a,b,c)$ where n is a non-zero integer. Another useful reduction is $(a,b,c) = (0, ac + b, c)$ and a third which is not quite so obvious is $(a,b,c) = (an, b + ac(1-n), c)$.

To continue the investigation of this system, the subsystem $< M, + >$ is considered. It should be clear that M is closed under + since the addition and multiplication of integers is closed. In order to verify the commutative and associative properties for + the following theorems are proven.

Theorem 4.1. If (a,b,c) , $(d,e,f) \in M$, then

$$(a,b,c) + (d,e,f) = (d,e,f) + (a,b,c).$$

Proof: By Definition 4.4,

$$(a,b,c) + (d,e,f) = (a + d,\ bf + ce,\ cf) = (d + a,\ fb + ec,\ fc)$$

since addition and multiplication of integers is commutative. But $(d + a,\ ec + fb,\ fc) = (d,e,f)$ by Definition 4.4. Therefore, $(a,b,c) + (d,e,f) = (d,e,f) + (a,b,c)$.

Theorem 4.2. If (a,b,c), (d,e,f), and $(g,h,i) \in M$, then $(a,b,c) + [(d,e,f) + (g,h,i)] = [(a,b,c) + (d,e,f)] + (g,h,i)$.

Proof: First, note that

$$\begin{aligned}(a,b,c) + [(d,e,f) + (g,h,i)] &= (a,b,c) + (d + g,\ ei + fh,\ fi)\\ &= (a + d + g,\ b(fi) + c(ei + fh,\ c(fi)\ )\\ &= (a + d + g,\ b(fi) +)c(ei) + c(fh,\ c(fi)\ )\\ &= (a + d + g,\ (bf)i + (ce)i + (cf)h,\ (cf)i\ )\\ &= (a + d + g,\ (bf + ce)i + (cf)h,\ (cf)i\ )\\ &= (a + d,\ bf + ce,\ cf) + (g,h,i) = [(a,b,c) + (d,e,f)] +\\ &\quad (g,h,i).\end{aligned}$$

A search for a representative for the identity and inverse elements for addition might logically lead the student to the following type reasoning. If (a,b,c), $(x,y,z) \in M$ and (x,y,z) is the additive identity, then $(a,b,c) + (x,y,z) = (a,b,c)$. Therefore,

$$(a + x,\ bz + cy,\ cz) = (a,b,c)$$

which implies that

$$[(a + x)cz + (bz + cy)]c = (ac + b)cz$$

or

$$(a + x)cz + (bz + cy) = (ac + b)z.$$

Hence,

$$acz + xcz + bz + cy = acz + bz.$$

So, $xcz + cy = 0$, which implies that $c(xz + y) = 0$, or that, $xz + y = 0$, since $c \neq 0$. If $xz + y = 0$, then $y = -xz$. Therefore, $(x, =xz, z)$ is a representative for the additive identity for arbitrary x and z, if $z \neq 0$. A simple representative of this class is $(0,0,1)$.

If (a,b,c), $(x,y,z) \in M$ and (x,y,z) is the additive inverse of (a,b,c), then $(a,b,c) + (x,y,z) = (0,0,1)$. Therefore, $(a + x, bz + cy, cz) = (0,0,1)$ which implies that $(a + x)cz + bz + cy = 0$. The problem now is to choose values for x,y,z such that the above statement is true and $(x,y,z) \in M$. Since (x,y,z) represents an equivalence class, there are many choices for x, y, and z. Probably the most obvious choice is to let $x = 0$ since every element in M can be reduced so that a zero appears in the first position. This approach would yield $acz + bz + cy = 0$ or $(ac + b)z = -cy$ which is certainly true if $y = ac + b$ and $z = -c$. Therefore, $(0, ac + b, -c)$ is a representative for the additive inverse.

Another approach to finding values for x, y, z in the above problem might begin by letting $z = c$ since $c \neq 0$ and z must be non-zero if $(x,y,z) \in M$. If $z = c$, then $(a + x)c^2 + bc + cy = 0$ or $(a + x)c + (b + y) = 0$. This statement is certainly true when $x = -a$ and $y = -b$. Therefore, another representative for the additive inverse for (a,b,c) would be $(-a, -b, c)$. Hence, $< M, + >$ is a commutative group.

The subsystem $< M, \cdot >$ is now investigated. It is immediately obvious from Definition 4.5 that M is closed under multiplication since multiplication and addition of integers is closed.

The following theorems verify that multiplication is commutative and associative.

Theorem 4.3. If (a,b,c), $(x,y,z) \in M$, then

$$(a,b,c) \cdot (x,y,z) = (x,y,z) \cdot (a,b,c).$$

Proof: First, note that

$(a,b,c)\cdot(x,y,z) = (ax,\ ayc + xbz + by,\ cz) = (xa,\ xbz + zyc + by,\ zc)$

since addition and multiplication of integers is commutative. But,

$$(xa,\ xbz + ayc + by,\ zc) = (x,y,z) \cdot (a,b,c)$$

which implies that $(a,b,c) \cdot (x,y,z) = (x,y,z) \cdot (a,b,c)$.

Theorem 4.4. If (a,b,c), (d,e,f), $(g,h,i) \in M$, then

$$(a,b,c) \cdot [\ (d,e,f) \cdot (g,h,i)\ ] = [\ (a,b,c) \cdot (d,e,f)\ ] \cdot (g,h,i).$$

Proof: From the definition of multiplication in M,

$$\begin{aligned}
(a,b,c) \cdot [(d,e,f) \cdot (g,h,i)] &= (a,b,c) \cdot (dg,\ dhf + gei + eh,\ fi) \\
&= (adg,\ a(dhf + gei + eh)c + dgbfi + b(dfg + gei + eh),\ cfi) \\
&= (adg,\ adhfi + ageic + aehc + dgbfi + bdgf + bgei + beh,\ cfi) \\
&= (adg,\ adhcf + gaeci + gdbfi + bgei + aech + dbfh + beh,\ cfi) \\
&= (adg,\ adcf + g(aec + dbf + be)i + (aec + dbf + be)h,\ cfi) \\
&= (ad,\ aec + dbf + be,\ cf) \cdot (g,h,i) \\
&= [(a,b,c) \cdot (d,e,f)] \cdot (g,h,i).
\end{aligned}$$

Hence, commutativity and associativity of multiplication hold for $< M, \cdot >$. A search for the multiplicative identity and inverse might lead the student to the following type reasoning. If (a,b,c), $(k,m,n) \in M$ and (k,m,n) is the multiplicative identity, then $(a,b,c) \cdot (k,m,n) = (a,b,c)$. But,

$$(a,b,c) \cdot (k,m,n) = (ak,\ amc + kbn + bm,\ cn) = (a,b,c).$$

So

$$[(ak)(cn) + amc + kbn + bm]c = (ac + b)cn$$

and

$$akcn + amc + kbn + bm = acn + bn.$$

Hence,

$$acn(k - 1) + bn(k - 1) + (ac + b)m = 0 \text{ and}$$

$(acn + bn)(k - 1) + (ac + b)m = (ac + b)(nk - n) + (ac + b)m =$ $(ac + b)[nk - n + m] = 0$ which implies that $ac + b = 0$ or $nk - n + m = 0$. If $(nk - n + m) = 0$, then $m = n(1 - k)$ and $(k,n(1 - k), n)$ is a representative for the multiplicative identity for arbitrary k and m, if $m \neq 0$. A simple representative of this class is $(1,0,1)$.

If (a,b,c), $(x,y,z) \in M$, $(a,b,c) \neq (0,0,1)$ and (x,y,z) is the multiplicative inverse of (a,b,c), then $(a,b,c) \cdot (x,y,z) = (1,0,1)$. Thus, $(ax, zcy + bxz + by, cz) = (1,0,1)$ which implies that $axcz + acy + bx + by = cz$ or $(ac + b)(xz + y) = cz$. Again, if $x = 0$, then $(ac + b)y = cz$ which is true when $y = c$ and $z = ac + b$. Hence, $(a,c,ac + b)$ is a representative for the multiplicative inverse of (a,b,c) if $(a,b,c) \neq (0,0,k)$.

Thus, the non-zero elements of M form a group under multiplication. The next theorem shows that multiplication distributes over addition in M.

Theorem 4.5. If (a,b,c), (d,e,f), $(g,h,i) \in M$, then $(a,b,c) \cdot [(d,e,f) + (g,h,i)] = [(a,b,c) \cdot (d,e,f)] + [(a,b,c) \cdot (g,h,i)]$.

Proof: Using the definition of addition in M,

$(a,b,c) \cdot [(d,e,f) + (g,h,i)] = (a,b,c)(d + g, ci + fh, fi)$

$= (a(d + g), a(ei + fh)c + (d + g)bfi + b(ei + fh), cfi)$

$= (ad + ag, aeic + afhc + dbfi + gbfi + bei + bfh, cfi)$

$= (ad + ag, (aeic + afhc + dbfi + gbfi + bei + bfh)c, cfic)$ since $(a,b,c) = (a, bn, cn)$.

Therefore,

$(ad + ag, aeic + afhc + dbfi + gbfi + bci + bfh, cfi)$

$= (ad + ag, aecci + bdfci + beci + cfahc + cfgbi + cfbh, cfci)$

$= (ad + ag, (aec + dbf + be)ci + cf(ahc + gbi + bh), cfci)$

$= (ad, aec + dbf + be, cf) + (ag, ahc + bgi + bh, ci)$

$= (a,b,c) \cdot (d,e,f) + (a,b,c) \cdot (g,h,i)$. Thus, multiplication distributes over addition in M.

Relative to the $< M, +, \cdot >$, it has been shown that (1) $< M, + >$ forms a commutative group, (2) $M \cap \{(0,0,k)\}$ forms a commutative group under multiplication, and (3) multiplication distributes over addition in M. Thus, the mathematical system $< M, +, \cdot >$ forms a field. One can now seek to discover if this field has some of the common characteristics of familiar fields. For example, one might seek answers to the following questions. Is $< M, +, . >$ an ordered field? Is $< M, +, . >$ isomorphic to a familiar field? These are important questions and will be considered in the following discussion.

Before one can investigate the possibility of $< M, +, . >$ forming an ordered field, an order relation must be defined on M.

Definition 4.6. $(a,b,c) \in M$ is in simple form iff $c > 0$ and $(b,c) = 1$.

Note that given an arbitrary representative for a class it is always possible to reduce this element to simple form. For example, $(3, 15, 21) = (3,5,7)$ and $(-21, 14, -35) = (-21, -2, 5)$.

Definition 4.7. If (a,b,c), (d,e,f) $\in$ M and (a,b,c), (d,e,f) are in simple form, then (a,b,c) $<_1$ (d,e,f) iff (ac + b)f < (df + e)c.

Definition 4.8. If (a,b,c), (d,e,f) $\in$ M and (a,b,c), (d,e,f) are in simple form, then (a,b,c) $>_1$ (d,e,f) iff (d,e,f) $<_1$ (a,b,c).

Theorem 4.6. "$<_1$" is an order relation on M.

Proof; Suppose that (a,b,c), (d,e,f), (g,h,i) $\in$ M and are in simple form. If (a,b,c) $<_1$ (d,e,f) and (d,e,f) $<_1$ (g,h,i), then (a,b,c) $<_1$ (g,h,i), that is, $<_1$ is transitive. To see that this is true, note that (a,b,c) $<_1$ (d,e,f) implies that (ac + b)f < (df + e)c and (d,e,f) $<_1$ (g,h,i) implies that (df + e)i < (gi + h)f. If (ac + b)f < (df + e)c, then (ac + b)fi < (df + e)ci since i > 0. If (df + e)i < (gi + h)f, then (df + e)ic < (gi + h)fc since c > 0. Since "<" is a transitive relation on the integers, (ac + b)fi < (gi + h)fc which implies that (ac + b)i < (gi + h)f since c > 0. But (ac + b)i < (gi + h)f implies (a,b,c) $<_1$ (g,h,i) and thus "$<_1$" is an order relation on M.

Definition 4.9. A field < F, +, . > is an ordered field if the following properties are satisfied:

(1) There exists a subset P, not containing the zero element, z, of F such that if x $\neq$ z, then one and only one of x and -x is in P.

(2) If x and y are in P, then (x + y) $\in$ P and (x.y) $\in$ P.

The elements of P are known as the positive elements of F and all other non-zero elements of F are known as the negative elements of F.

Theorem 4.7. < M, +, ., $<_1$ > is an ordered field.

Proof: Define P and N as follows:

$P = \{(a,b,c) \in M \mid (a,b,c) \text{ is in simple form and } (a,b,c) >_1 (0,0,1)\}$

$N = \{(a,b,c) \in M \mid (a,b,c) \text{ is in simple form and } (a,b,c) <_1 (0,0,1)\}$.

If $(x,y,z) \in M$ and (x,y,z) is in simple form with $(x,y,z) \neq (0,0,1)$, then $(x,y,z) \in P$ or $(x,y,z) \in N$ since $(x,y,z) >_1 (0,0,1)$ or $(x,y,z) <_1 (0,0,1)$ but not both. If $(a,b,c) \in P$ and $(d,e,f) \in P$, then $(a,b,c) >_1 (0,0,1)$ and $(d,e,f) >_1 (0,0,1)$ or $(ac + b) > 0$ and $(df + e) > 0$ which implies $(ac + b)f > 0$ and $(df + e)c > 0$ since $f > 0$ and $c > 0$.

Therefore,

$$[(ac + b)f + (df + e)c] > 0$$

which implies that

$$(acf + dcf + bf + ce) > 0$$

or that

$$[(a + d)cf + df + ce] > 0$$

which in turn implies that

$$(a + d,\ df + ce,\ cf) = [(a,b,c) + (d,e,f)] >_1 (0,0,1).$$

Hence,

$$(a,b,c) + (d,e,f) \in P.$$

Similarly, if (a,b,c), $(d,e,f) \in P$, then $(ac + b) > 0$ and $(df + e) > 0$ which implies that $(ac + b)(df + e) > 0$ or that

$$(adcf + aec + bdf + bc) > 0.$$

Therefore,

$(ad,\ aec + bdf + be,\ cf) = [(a,b,c) \cdot (d,e,f)] >_1 (0,0,1)$ which implies that $(a,b,c) \cdot (d,e,f) \in P$. Thus, $< M, +, \cdot <_1 >$ is an ordered field.

Definition 4.10. If $(a,b,c) \in M$ and n is a positive integer, then $n(a,b,c)$ is the nth natural multiple of (a,b,c), that is, $n(a,b,c) = (a,b,c) + (a,b,c) + \ldots + (a,b,c)$ (n summands of (a,b,c)).

Definition 4.11. An ordered field F is an Archemedian ordered field iff for any two positive elements x and y in F, there exists a positive integer n such that $nx > y$.

Theorem 4.8. If $(a,b,c) \in M$, then $n(a,b,c) = (na, nb, c)$.

Proof: This theorem is proven by induction. It is true for $n = 1$ since $(a,b,c) = (a,b,c)$. Assume that it is true for $n = k$, that is, $k(a,b,c) = (ka, kb, c)$. Now show the statement is true for $n = k + 1$. First, note that $(k + 1)(a,b,c) = k(a,b,c) + (a,b,c) = (ka, kb, c) + (a,b,c)$ by the induction hypothesis.

But

$$\begin{aligned}(ka, kb, c) + (a,b,c) &= (ka + a, kbc + bc, c^2)\\ &= ((k + 1)a, (k + 1)bc, c^2)\\ &= ((k + 1)a, (k + 1)b, c)\end{aligned}$$

since $(a,b,c) = (a, bn, cn)$. Therefore, the statement is true for every n.

Theorem 4.9. $< M, +, \cdot, <_1 >$ is an Archemedian ordered field.

Proof: Without loss of generality, suppose that $(a,b,c), (d,e,f) \in P$ and that $(a,b,c) <_1 (d,e,f)$. If there exists a positive integer n such that $n(a,b,c) >_1 (d,e,f)$, then $(nac + nb)f > (df + e)c$ or $nf(ac + b) > (df + e)c$. Let $n = (df + e)(c + 1)$ and then $(df + c)(c + 1)f(ac + b) > (df + e)c$ or $(c + 1)f(ac + b) > c$ which is certainly true since $f > 0$ and $ac + b > 0$. Thus, given that

(a,b,c), $(d,e,f) \in P$, then there exists a positive integer n such that $n(a,b,c) >_1 (d,e,f)$ which implies that $< M, +, \cdot, <_1 >$ is an Archemedian ordered field.

It is a historical fact that often independent studies have been made of two or more mathematical systems, and later these systems have been recognized to be essentially the same system. This phenomenon was noted in the study of groups in Chapter III. As noted earlier, these systems are referred to as being isomorphic.

Definition 4.11. Two mathematical systems S and T are called isomorphic if there is a one-to-one correspondence between the elements, relations, operations of S and T such that under this correspondence of elements all relations and operations are preserved.

To say that operations are preserved by the correspondence, one means that if a corresponds to a' and b corresponds to b', with $a,b \in S$ and $a', b' \in T$, it follows that ab corresponds to a'b'. In order to further clarify this idea of a correspondence, it is often helpful to think of this correspondence as a function from S to T.

Definition 4.12. Let f be a function defined on S. f is said to be one-to-one on S iff, for every x and y in S, $f(x) = f(y)$ implies that $x = y$.

Definition 4.13. If f is a function such that $f: S \rightarrow T$. Then f is a function of S onto T iff $f(S) = T$.

Definition 4.13. If S and T are two mathematical systems such that for each operation and relation in S there is a corresponding relation or operation in T, and f is a one-to-one function from S onto T which preserves the relations and operations of S, then f is an isomorphism from S to T.

As a familiar example of an isomorphism between two mathematical systems, consider the set S of positive real numbers, expressed as powers of 10, with the binary operation of ordinary multiplication, and the set T of all real numbers with the binary operation of ordinary addition. If f is a function from S to T defined by $f(10^x) = x$, then f is a one-to-one function from S onto T. Further, note that the operations are preserved since $f(10^x \cdot 10^y) = f(10^{x+y}) = x + y = f(10^x) + f(10^y)$. Hence, f is an isomorphism. This isomorphism is commonly referred to as the common logarithm function.

It is now possible to use the concept of isomorphism to reveal that the system $< M, +, . >$ is isomorphic to the rational numbers, Q.

Theorem 4.10. $< M, +, . >$ is isomorphic to the rational numbers, Q.

Proof: Let $f: M \rightarrow Q$ such that $f(a,b,c) = \frac{ac + b}{c}$. f is a one-to-one function since if $f(a,b,c) = f(d,e,f)$, then

$$\frac{ac + b}{c} = \frac{df + e}{f}$$

or $(ac + b)f = (df + e)c$ which implies that $(a,b,c) = (d,e,f)$. f is also onto since for any $a/b \in Q$, there exists an element $(x,y,z) \in M$ such that $f(x,y,z) = a/b$; namely; $(x,y,z) = (0,a,b)$. f also preserves the operations of addition and multiplication since

$$\begin{aligned} f[(a,b,c) + (d,e,f)] &= f(a + d,\ bf + ce,\ cf) \\ &= \frac{acf + dcf + bf + ce}{cf} \\ &= \frac{ac + b}{c} + \frac{df + e}{f} \end{aligned}$$

$$= f(a,b,c) + f(d,e,f).$$

Further,

$$\begin{aligned} f[(a,b,c) \cdot (d,e,f)] &= f(ad,\ aec + bdf + be,\ cf) \\ &= \frac{adcf + aec + dbf + be}{cf} \\ &= \frac{ac(df + e) + b(df + e)}{cf} \\ &= \frac{(ac + b)(df + e)}{cf} \\ &= \frac{ac + b}{c} \cdot \frac{df + e}{f} \\ &= f(a,b,c) \cdot f(d,e,f). \end{aligned}$$

Thus, the unfamiliar field $< M, +, \cdot >$ is nothing more than the field of mixed numbers disguised as ordered triples of integers. This example provides a situation in which one can illustrate and reinforce several of the fundamental concepts of abstract algebra. The beauty of this system lies in the fact that the student is placed in somewhat of a strange situation since he loses his intuition and must rely on his understanding of the concepts involved. Hopefully, this artificial situation is both intriguing and rewarding for the student.

CHAPTER V

SOME FINITE GEOMETRIES

An interesting question for a mathematics class to consider might be: "What is a point?" Typical responses such as: "A point is a position in space," "A point has no length or width," or "A point is the intersection of two lines", each fail as a definition. If the discussion persisted, the responses would more than likely dwindle until the class retreated into a frustrated silence. What is important here is that only rarely will any student take issue with the legitimacy of the question. It seems quire reasonable to the student that after studying plane geometry for a year he should be able to define a point in the same sense that he was able to define a triangle or a circle. However, the question is not legitimate since the word "point" in geometry is not defined in the usual sense. The words "point," "line," "on," and some others are primitive notions or undefined terms of the system. They are taken as undefined in order to avoid circularity of definitions.

The axioms for a given system merely specify the behavior of the undefined terms; however, they do not specify the meaning of the undefined terms. This is an important consideration which is often overlooked. Wylie notes that the logical defects in the word of Euclid placed particular emphasis on the role of undefined terms and axioms or postulates in the development of a mathematical system.[1] The words axiom and postulate have the same meaning and are used interchangeably.

The study of miniature or finite geometries provides an excellent vehicle for the study of abstract axiomatic systems. MacNeish defines a finite geometry as a geometry based on a set of postulates, undefined terms, and undefined relations which limits the set of all points and lines to a finite number.[2] The elements "point" and "line" are undefined terms. Golos points out that in some of the modern systems the words "point" and "line" are replaced by nonsense words such as "abba" and "dabba" to stress the fact that the words "point" and "line" are truly undefined.[3] Thus, whatever "points" are, they can be considered as elements in some universal set. A "line" is regarded as some undefined subset of the universal set.

It is customary to represent points by capital letters and lines by small letters. However, it is much more consistent with set notation to represent sets of elements by capital letters and elements of a set by small letters. Thus, lines are represented by capital letters A, B, C, ... and points are represented by small letters a, b, c, . . ., z. If a point belongs to a subset called a line, then the point is said to be on that line. Conversely, the line is on or passes through the point. Two lines that have a point in common are said to intersect in that point.

Historically, the study of foundations of Euclidean geometry led to the axiomatic approach and its importance in all branches of mathematics. The axiomatic approach involves selecting a set of undefined terms and a set of axioms containing them. The system is developed by deducing theorems from these axioms or from previously deduced theorems by means of the chosen logic. Thus, a theorem is a logical consequence of the axioms. The axiom system as such is meaningless and the question of the "truth" of the axioms is irrelevant. If meanings are assigned to each of the undefined terms in such a way that the axioms are judged to be "true", then the axiom set is said to be interpreted. A model of a postulational system is obtained when each undefined term is interpreted.[4] Golos suggests that there are three important concepts usually associated with an axiomatic system: consistency, independence, and completeness.

Definition 5.1. An axiom system is consistent iff there do not exist in the system any two axioms, any axiom and theorem, or any two theorems that are contradictory.

Consistency is the most important and the most fundamental property of a set of axioms. The most successful test for consistency is the method of models. If there exists a model for a set of axioms, then the set is consistent.

Definition 5.2. An axiom is independent from the other axioms of the system if it cannot be derived from these axioms. An axiom system is independent if each axiom is independent.

To prove that a given postulate is independent of the other postulates of the system, it is sufficient to construct a model in which the given postulate is not valid, but all other postulates of the system are valid. This is not always easy to do, and can be quite a lengthy process. Eves and Newsom point out that independence of a postulational system is by no means necessary, and the system is not invalidated just because it lacks independence.[6] Mathematicians prefer that a postulational system be independent, thereby minimizing the number of necessary assumptions.

In developing an axiomatic system, the set of axioms should be inclusive enough to imply the truth or falsity of any possible statement using these undefined terms and relations. Clearly, if a statement cannot be classified as true or false with respect to the existing system, it can only be because the axiomatic system is lacking necessary axioms. This leads to the concept of completeness of an axiom set.

Definition 5.3. An axiom system is complete if it is impossible to add an independent axiom which is consistent with the given set of axioms and which does not contain any new undefined terms.

It is often difficult to prove directly that a given set of axioms is complete. The test for completeness relies on some rather sophisticated concepts that are beyond the scope of this presentation. A complete discussion of consistency, independence, and completeness is given by Blumenthal.[7]

To introduce the idea of a finite geometry, consider System I whose undefined elements, point and line, satisfy the following postulates.

System I

P1: There exist exactly three distinct points.

P2: Two distinct points determine a unique line.

P3: Not all points are on the same line.

P4: Two distinct lines determine at least one point.[8]

The finite geometry determined by this postulational system might well be considered the simplest non-trival finite geometry. A model for this system is given in Figure 39. Clearly, this model illustrates the consistency of the system.

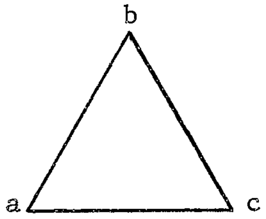


Figure 39

The independence of the postulational system is proven as follows:

Independence of P1: A rectangle suffices to illustrate the independence of this postulate since P1 is not satisfied by this model, but the remaining three postulates are satisfied.

Independence of P2: Three points and no lines will satisfy all the postulates except P2.

Independence of P3: If a model is constructed with one line and three points on it, then P3 is not true, but the other three postulates hold.

Independence of P4: Figure 40 illustrates two lines with no points in common. Then, P1, P2, and P3 are satisfied while P4 is not.

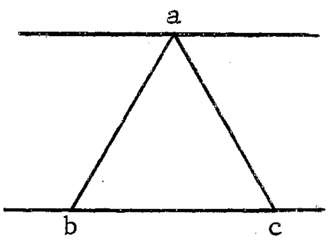


Figure 40

Thus, P1, P2, P3, and P4 form a consistent set of axioms and each axiom is independent. A theorem that might be deduced from this system is that there are exactly three lines.

Another example of a finite geometry consists of a definition and four postulates which are given below in System II.

System II

Definition 1: Two lines are parallel iff no point lies on both lines.

P1: There is at least one point.

P2: Every line is a set of exactly two points.

P3: Every point lies on exactly two lines.

P4: To a given line there are exactly three parallel lines.[9]

To establish the consistency of this postulate set, the model shown in Figure 41 consisting of six points and six lines can be used.

A figure with no points and no lines, the null set, can be used to establish the independence of P1. Figures 42, 43, and 44 illustrate the independence of postulates P2, P3, and P4, respectively.

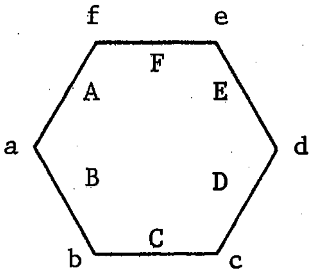


Figure 41

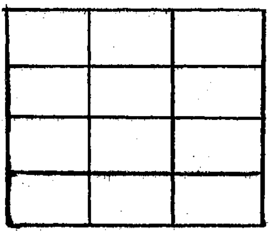


Figure 42

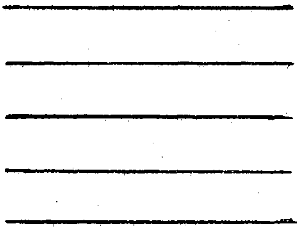


Figure 43

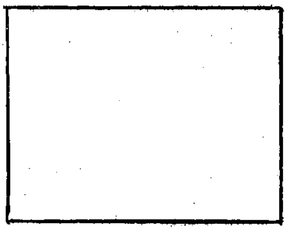


Figure 44

Using the postulates for System II, it is possible to verify each of the following theorems.

<u>Theorem 5.1</u>. If there are two distinct points, a and b, lying on both L and K, then L = K.

Proof: Suppose the points a and b both lie on lines L and K, where $a \neq b$. Then, L = ab and K = ab by P2. Therefore L = K.

<u>Theorem 5.2</u>. There is at least one line.

Proof: By P1, there is a point and from P3, every point lines on exactly two lines. Hence, there exists at least one line.

Theorem 5.3. To a given line there are exactly two non-parallel lines.

Proof: Let L be the given line. Then, L = ab, where $a \neq b$, by P2. There are lines M and N, distinct from L, containing a and b respectively, by P3. But M and N are not parallel to L.

Theorem 5.4. There are exactly six lines.

Proof: From Theorem 5.2, there is a line. Theorem 5.3 implies that there are two lines not parallel to a given line and P4 implies that there are three lines parallel to a given line. Therefore, there are six lines.

Theorem 5.5. There are exactly six points.

Proof: From Theorem 5.4, there are six lines. P2 guarantees that each line contains two points and P3 insures that each point lies on two lines. Hence, there are exactly six points.

The next example of a finite geometry to be considered is the seven-point seven-line finite geometry. The postulational system for this geometry is given below in System III.

System III

P1: If a and b are distinct points of S, then there exists at least one line containing both a and b.

P2: If a and b are distinct points of S, then there is not more than one line containing both a and b.

P3: Any two lines have at least one point of S in common.

P4: There exists at least one line.

P5: Every line contains at least three points of S.

P6: Not all points are on the same line.

P7: No line contains more than three points of S.[10]

A model that will demonstrate consistency is the set of seven letters a, b, c, d, e, f, g arranged in seven lines with three points on each line. Figure 45 illustrates this configuration where the vertical columns represent the lines.

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

Figure 45

Figures 46 and 47 illustrate two geometric models that also satisfy this postulate set.

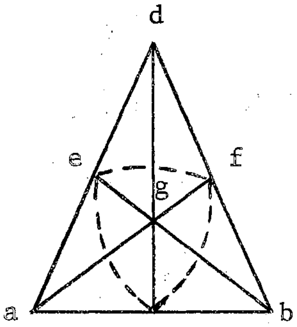


Figure 46

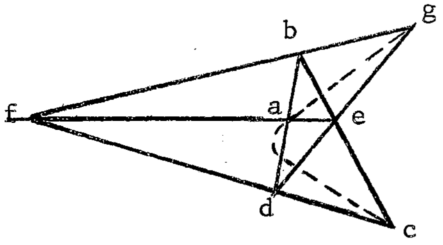


Figure 47

To establish independence, consider the following models:

Independence of P1: Let the set S consist of the points a, b, c, d, e with the lines dae and dbc. P1 does not hold since there is no line with both a and b as elements; however, the remaining six postulates hold.

Independence of P2: Let S be a tetrahedron, Figure 48, abcd where the faces represent lines.

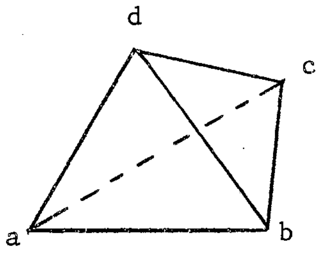


Figure 48

Independence of P3: Let S consist of nine points and twelve lines as shown in Figure 49, where the vertical columns represent lines. Note that P3 is not true, but the remaining postulates are true.

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

Figure 49

Independence of P4: For a single point a, P4 does not hold; however, the remaining postulates are fulfilled vacuously.

Independence of P5: A triangle with a, b, c as vertices satisfies all the postulates but P5.

Independence of P6: A line containing three points a, b, c will not satisfy P6 but the other postulates are valid.

Independence of P7: Let S consist of a thirteen-point thirteen-line array with four points on each line. The vertical columns again represent the lines. All the postulates but P7 are satisfied by the configuration shown in Figure 50.

1	2	3	4	5	6	7	8	9	10	11	12	13
2	3	4	5	6	7	8	9	10	11	12	13	1
4	5	6	7	8	9	10	11	12	13	1	2	3
10	11	12	13	1	2	3	4	5	6	7	8	9

Figure 50

What theorems can be proved in this geometry? MacNeish suggests that the duals of the postulates may be proven as theorems.[11]

Definition 5.4. Two statements which differ only in the interchange of the words "point" and "line" are said to be duals of each other.

For example, Postulate P1 and P3 are duals of each other.

Theorem 5.6 (Dual of P2). Two distinct lines have only one point in common.

Proof: Any two lines have at least one point in common by P3. Assuming that these two lines have two points in common contradicts P2. Therefore, the two lines have exactly one point in common.

Theorem 5.7 (Dual of P6). All lines do not pass through the same point.

Proof: The existence of at least one line is guaranteed by P4, every line contains three points by P5 and P7, and not all points are on the same line by P6. Now, let L be the line determined by the points a, b, and c. Any line connecting a point d to any point of the line abc must contain another point since each line contains exactly three points. But there is exactly one line containing any two points of S by Theorem 5.1. Therefore, all lines do not pass through the same point.

Theorem 5.8 (Dual of P4). There exists at least one point.

Proof: This theorem is an immediate consequence of P4 and P5.

Theorem 5.9. There are exactly seven points.

Proof: There exists at least one line by P4 and this line contains three points, a, b, and c. By P6, not all the points are on the same line. Let d be the point not on abc. The line joining a and d must contain three points. Call this third point e. Neither b or c can be on line ade since there are exactly three points on each line. Similarly, there is a line bdf. Thus, there are three lines abc, ade, and bdf which imply there are at least six points. It is possible to connect a with either b, c, d, or e. Since a must be connected with f, and b, c, d, and e cannot be used, then there must be a seventh point g. Hence, afg is a line. Suppose that there is an eighth point h, then the line connecting a and h could not have a point in common with any of the lines without violating Theorem 5.6. Thus, there are exactly seven points.

Theorem 5.10 (Dual of Theorem 5.9). There are exactly seven lines.

Proof: From the proof of Theorem 5.9, the lines are those illustrated in Figure 51.

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

Figure 51

Thus, there are exactly seven lines.

Theorem 5.11. Exactly three lines pass through every point.

Proof: This theorem is an immediate consequence of Theorems 5.9 and 5.10.

The next finite geometry to be considered is Young's nine-point twelve-line geometry. The postulates for this geometry are given below in System IV.

System IV

P1: If a and b are distinct points of S, then there exists one line containing both a and b.

P2: If a and b are distinct points of S, then there exists not more than one line containing a and b.

P3: Given a line L not containing a point a, then there exists one line containing a and not containing any point of L.

P4: Given a line L not containing a point a, then there exists not more than one line containing a and not containing any point of L.

P5: Every line contains at least three points.

P6: Not all points are contained by the same line.

P7: There exists at least one line.

P8: No line contains more than three points.[12]

A model demonstrating consistency for this postulate set is given in Figure 52.

1	1	1	1	2	2	2	3	3	3	4	7
2	4	5	6	5	4	6	4	5	6	5	8
3	7	9	8	8	9	7	8	7	9	6	9

Figure 52

A geometric model serving the same purpose is given in Figure 53.

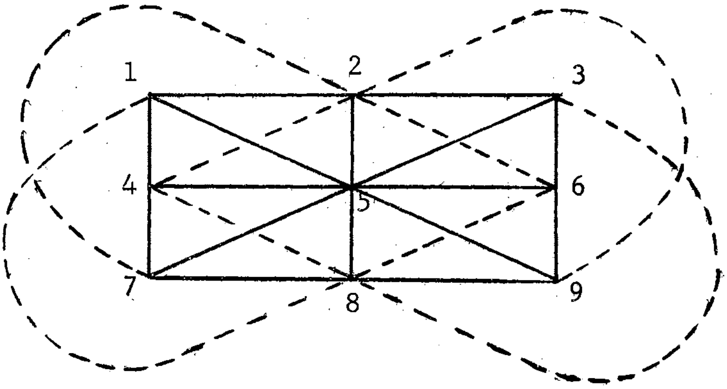


Figure 53

The independence of this postulate set is shown as follows:

Independence of P1: Two lines, abc and def, satisfy all postulates except P1.

Independence of P2: The arrangement of six points taken three at a time to form twenty lines illustrates the independence of P2 since every postulate is satisfied except P2. This arrangement is illustrated in Figure 54.

1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	3	3	3	4
2	2	2	2	3	3	3	4	4	5	3	3	3	4	4	5	5	4	4	5	5
3	4	5	6	4	5	6	5	6	6	4	5	6	5	6	6	6	5	6	6	6

Figure 54

Independence of P3: The seven-point finite geometry given in System III will suffice to show the independence of P3.

Independence of P4: An array of thirty-five lines, formed from fifteen points taken three at a time given in Figure 55 serves as a model to illustrate the independence of P4.

1	2	3	4	5	6	7	8	9	10	11	12
4	5	6	7	8	9	10	11	12	13	14	15
5	6	7	8	9	10	11	12	13	14	15	1

13	14	15	1	2	3	4	5	6	7	1	2
1	2	3	3	4	5	6	7	8	9	8	9
2	3	4	9	10	11	12	13	4	15	10	11

3	4	5	6	1	2	1	2	3	4	5
10	11	12	13	7	8	6	7	8	9	10
12	13	14	15	14	15	11	12	13	14	15

Figure 55

Independence of P5: A complete quadrilateral as illustrated in Figure 56 serves as a model to illustrate the independence of P5.

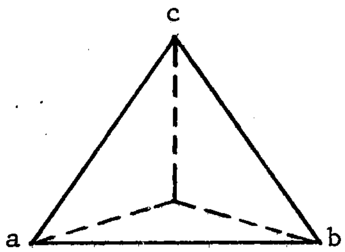


Figure 56

Independence of P6: A single line of three points does not satisfy P6, but does satisfy the other postulates. Note that P3 and P4 are satisfied vacuously.

Independence of P7: A single point and no lines satisfies all of the postulates except P7.

Independence of P8: Plane Euclidean geometry suffices to show independence of this postulate.

Some theorems that result from this finite geometry are given below. The proofs of these theorems are quite simple and follow the patterns used in the previous sections.

Theorem 5.12. If a and b are distinct points of S, then there exists exactly one line containing both a and b.

Theorem 5.13. Given a line L not containing a point a, there exists exactly one line containing a and not containing any point of L.

Theorem 5.14. Every line contains exactly three points.

Theorem 5.15. There exists exactly nine points.

Theorem 5.16. There exists exactly twelve lines.

Theorem 5.17. Every line has precisely two lines parallel to it.

System V is the postulate set for the Pappas finite geometry.

System V

P1: There exist at least one line.

P2: Not all points are on the same line.

P3: Given two distinct points, there is at most one line joining them.

P4: Every line contains at least three points.

P5: No line contains more than three points.

P6: Given a line and a point not on that line, there exists a line containing the given point which has no point in common with the first line.

P7: Given a line and a point not on that line, there exists not more than one line containing the given point which has one point in common with the first line.

P8: Given a point and line not containing that point, there exists a point contained in the given line which is not on any line with the first point.

P9: Given a point and a line not containing the point, there exists not more than one point contained in the given line which is not on any line with the first point.[13]

A model illustrating the consistency of this postulational system consists of nine points and nine lines. Figure 57 illustrates nine points and nine lines in an array where the vertical columns represent lines.

1	1	1	2	2	3	3	4	7
2	4	5	4	6	5	6	5	8
3	8	9	7	9	7	8	6	9

Figure 57

A geometric figure illustrating the consistency of this postulate is given in Figure 58.

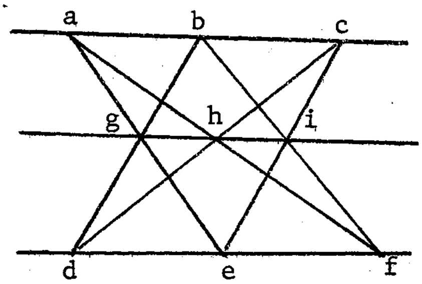


Figure 58

The independence of this postulate set can be shown as follows:

<u>Independence of P1</u>: A single point does not satisfy P1, but the other postulates are fulfilled vacuously.

<u>Independence of P2</u>: A single line containing three points, a, b, c, does not satisfy P2; however, the other postulates remain true.

<u>Independence of P3</u>: The faces of an octahedron where the faces represent lines as shown in Figure 59 illustrate the independence of P3.

1	1	1	1	6	6	6	6
2	2	4	3	2	2	5	3
3	4	5	5	3	4	4	5

Figure 59

Figure 60 gives a geometric model which also shows the independence of P3.

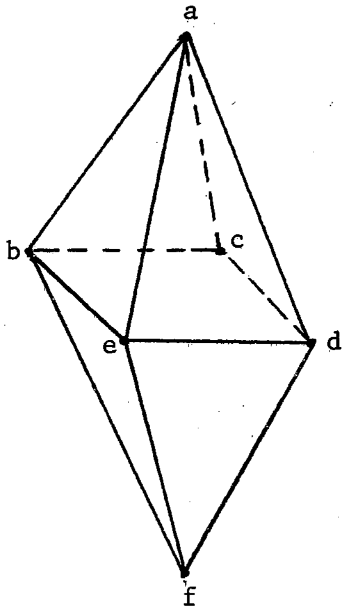


Figure 60

Independence of P4: A simple quadrilateral abcd satisfies all the postulates except P4.

Independence of P5: An arrangement of sixteen points and sixteen lines with four points on a line serves as a model to illustrate the independence of P4. This arrangement is illustrated in Figure 61.

Independence of P7: A figure with six points and four lines with three points on a line as shown in Figure 62 serves as a model to illustrate the independence of P7.

1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
5	6	7	8	5	6	7	8	5	6	7	8	5	6	7	8
9	10	11	12	10	9	12	11	11	12	9	10	12	11	10	9
13	14	15	16	16	15	14	13	14	13	16	15	15	16	13	14

Figure 61

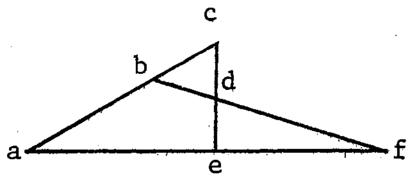


Figure 62

Independence of P8: The nine-point twelve-line geometry determined by System IV serves as a model to establish the independence of P8.

Independence of P9: Two non-intersecting straight lines, abc and def, satisfy the first eight postulates but not P9.

Some theorems arising from the Pappas finite geometry are:

Theorem 5.18. Every line contains exactly three points.

Theorem 5.19. Given a line and a point not on that line, there exists exactly one line containing the given point which has no point in common with the first line.

Theorem 5.20. Given a point and a line not containing that point, there exists exactly one point contained in the given line which is not on any line with the first point.

Theorem 5.21. There exists at least one point.

Theorem 5.22. Not all lines pass through the same point.

Theorem 5.23. Two distinct lines have at most one point in common.

Theorem 5.24. At least three lines pass through each point.

Theorem 5.25. At most three lines pass through each point.

Theorem 5.26. Exactly three lines pass through each point.

The Pappas finite geometry is treated in some detail by Richardson.[14]

To this point in the discussion the finite geometries considered have had only a slight resemblance to the familiar Euclidean geometry; however, many of the Euclidean plane geometry theorems can be proved in the Cundy 25-point geometry. This geometry is defined by the postulates given in System VI.

System VI

P1: There is one and only one line joining any two points.

P2: Two lines meet in one point unless they are parallel.

P3: Through any point there is one and only one point line parallel to a given line.

P4: Through any point there is one and only one line perpendicular to a given line.[15]

Many of the theorems from Euclidean geometry expressed in terms of this geometry can be proved. To facilitate the discussion of this geometry, 25 letters are arranged in a special way and presented in Figure 63. Using this table, it is now possible to state definitions which are basic to the development of this geometry.

a b c d e	a i l t w	a h o q x
f g h i j	s v e h k	n p w e g
k l m n o	g o r u d	v d f m t
p q r s t	y c f n q	j l s u c
u v w x y	m p s b j	r y b i k
Block 1	Block 2	Block 3

Figure 63

Definition 5.5. A straight line is any row or any column of the three blocks in Figure 63.

For example, fghij and hpdly are lines. Note that there are a total of 30 lines in this geometry and each line is determine by exactly five points.

Definition 5.6. The distance between two points is defined as the least number of steps separating the points on the line which contain them.

For example, the distance between a and i on the line ailtw is 1 and the distance between w and b on owfsb is 2. (See Figure 64.)

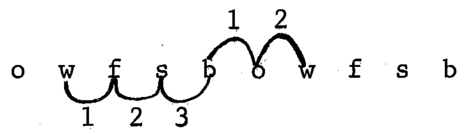


Figure 64

Numerals such as 1 and 2 will be used to designate row distances, while primed numerals such as 1' and 2' will designate column distances.

Definition 5.7. A line segment, a pair of points, is called congruent to another line segment when both segments occur in rows (or both in columns) and if the number of steps between the points is the same in both segments.

For example, line segment ai is congruent to line segment sr.

Definition 5.8. If two lines have a single point in common, then that point is called the point of intersection of the two lines.

Definition 5.9. Two straight lines are parallel iff they have no points in common.

Thus, fghij || klmno and ifocp || lerfx. Note that for lines to be parallel they must both be rows (or both columns) from the same block.

Definition 5.10. Two or more lines are said to be concurrent if they intersect in a point.

Definition 5.11. Any three non-collinear points determine a triangle. The sides are segments determined by taking the triple of points in pairs.

Thus, osu is a triangle where the segments os, su, and ou determine the lines klmno, pqrst, and uvwxyz, respectively. Cundy notes that there are 2000 triangles in this geometry of which 1200 are scalene right-angled triangles. He also concluded that there were 600 isosceles triangles and 200 equilateral triangles.[16] For example, abf is isosceles right-angled triangle since ab = 1, af = 1', bf = 2', and ab $\perp$ af. Note that Δabi is an equilateral triangle and Δabh is an isosceles triangle.

Definition 5.12. If there is a triple of points on the same line such that the number of steps from the first to the second is the same as the number of steps from the second to the third, then the second point is called the midpoint of the segment determined by the first and third points.

Hence, d is the midpoint of the segment ab since ad = bd.

Definition 5.13. A circle is a set of points such that any one of them taken with the center determines a segment which is congruent to every other such segment.

For example, lnjpft forms a circle with center m since ml = mn = mj = mp = mf = mt. Cundy found that there are 100 circles for the 25 centers and 4 possible radii.[17]

As mentioned earlier, many of the theorems in Euclidean geometry expressed in terms of the 25-point geometry are true. However, a rigorous proof of these theorems is a very laborious task. In Euclidean geometry it is possible to select an arbitrary geometric figure satisfying the hypothesis of the theorem and then deducing the conclusion using the axioms and previous theorems. In the 25-point geometry, selecting a geometric figure arbitrarily has very little meaning. Thus, a rigorous proof of a theorem would involve an argument by cases until the set under consideration is exhausted.

In the proofs that follow, only one case is illustrated. Therefore, these proofs are by no means complete. They do, however, offer some indication why an Euclidean geometry theorem is true in the 25-point geometry.

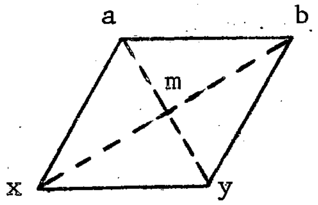


Figure 65

Theorem 5.27. The diagonals of rhombus are perpendicular.

Proof: Consider the rhombux abyx shown in Figure 65. The diagonal ay determines the line asgym and the diagonal bx determined the line mpxbj. The point of intersection is m and the two lines are perpendicular since asgym is a column and mpxbj is a row.

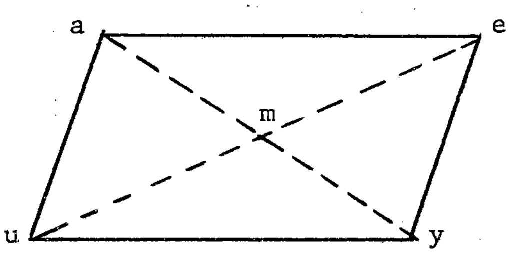


Figure 66

Theorem 5.28. The diagonals of a parallelogram bisect each other.

Proof: Consider the parallelogram in Figure 66 determined by aeuy. The diagonals ay and ue determine the lines asgym and qemui, respectively. But am = ym = em = 1'. Therefore, the diagonals bisect each other.

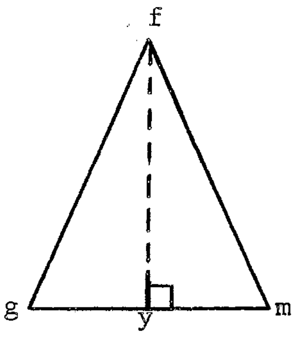


Figure 67

Theorem 5.29. The altitude to the base of an isosceles triangle bisects the base.

Proof: Consider △ abj shown in Figure 67. Note that gf = fm = 1 and gm = 2'. The base is asgym and the vertex is f. Also, ycfn ⊥ asgyn at y. But gy = ym = 1 which implies that the altitude ycfnq bisects af.

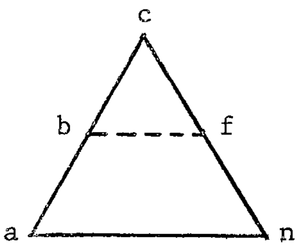


Figure 68

Theorem 5.30. The segment joining the midpoints of two sides of a triangle is parallel to the third side.

Proof: Consider △ acn shown in Figure 68. Notice that b and f are midpoints of the sides ac and cn, respectively. The third side of the triangle is anvjr and owfsb is the line determined by the segment bf. Thus, anvjr || owfsb.

There are many other Euclidean theorems that hold in this geometry and it is an intriguing exercise to hunt for such theorems. The theorems listed below make interesting exercises and were suggested by Coxford.[18]

<u>Theorem 5.31</u>. The segments determined by the midpoints of the sides of a parallelogram form a parallelogram.

<u>Theorem 5.32</u>. The altitudes of a triangle meet in a point called the orthocenter.

<u>Theorem 5.33</u>. The perpendicular bisectors of the sides of a triangle meet in a point called the circumcenter.

<u>Theorem 5.34</u>. For isosceles and equilateral triangles there are circles whose centers are the midpoint of the segment joining the orthocenters and the circumcenters, and which pass through the feet of the altitudes, the midpoints of the sides, and the midpoints of the segments joining the vertices of the triangles to the orthocenters.

<u>Theorem 5.35</u>. The orthocenter, circumcenter, and centroid are collinear; and the distance from the orthocenter to the centroid is twice the distance from the centroid to the circumcenter.

For the reader who is interested in more advanced ideas in this geometry, see the articles by Cundy[19] and Heidlege.[20]

Hopefully, this development of finite geometries illustrates that many of the basic properties of axiomatic systems and geometric systems can be introduced through the study of finite geometries. Additional references for other finite geometries and related topics are given in the Appendix.

FOOTNOTES

[1] C. R. Wylie, *Foundations of Geometry* (New York, 1964), p. 29.

[2] H. F. MacNeish, "Four Finite Geometries," *American Mathematical Monthly*, XLIX (January, 1942), p. 15.

[3] E. B. Golos, *Foundations of Euclidean and Non-Euclidean Geometry* (New York, 1968), p. 21.

[4] L. M. Blumenthal, *A Modern View of Geometry* (San Francisco, 1961), p. 39.

[5] Golos, p. 38.

[6] H. Eves and C. V. Newsom, *An Introduction to the Foundations and Fundamental Concepts of Mathematics* (New York, 1958), p. 167.

[7] Blumenthal, pp. 40-47.

[8] B. E. Meserve, *Fundamental Concepts of Geometry* (Cambridge, Massachusetts, 1955), p. 12.

[9] Committee on the Undergraduate Program, *Elementary Mathematics of Sets with Applications* (Berkeley, 1958), p. 118.

[10] MacNeish, p. 15.

[11] Ibid., p. 16.

[12] Ibid., p. 18.

[13] Ibid., p. 20.

[14] M. R. Richardson, *Fundamentals of Mathematics* (New York, 1941), p. 450.

[15] H. M. Cundy, "25-Point Geometry," *Mathematical Gazette*, XXXVI (September, 1952), p. 159.

[16] Ibid., p. 160.

[17] Ibid., p. 163.

[18] A. F. Coxford, "Geometric Diversions: a 25-Point Geometry," *The Mathematics Teacher*, LVII (December, 1964), pp. 563-564.

[19] Cundy, pp. 158-166.

[20] Martha Heidlage, "A Study of Finite Geometry," The Pentagon, XXII (Fall, 1963), pp. 18-27.

CHAPTER VI

SOME INTERESTING APPLICATIONS OF GRAPH THEORY

The theory of graphs is one of the few fields of mathematics with a definite birthdate. In 1736 at the age of 20, the Swiss mathematician Leonhard Euler presented the first paper on graphs to the Russian Academy of Science. Euler began his paper by discussing a then famous puzzle, the so-called Königsberg Bridge Problem.[1]

Königsberg stands on the banks of the River Pregel in East Prussia. In the center of the river lies the small island of Kneiphof and spanning the river are seven bridges as shown in Figure 69.

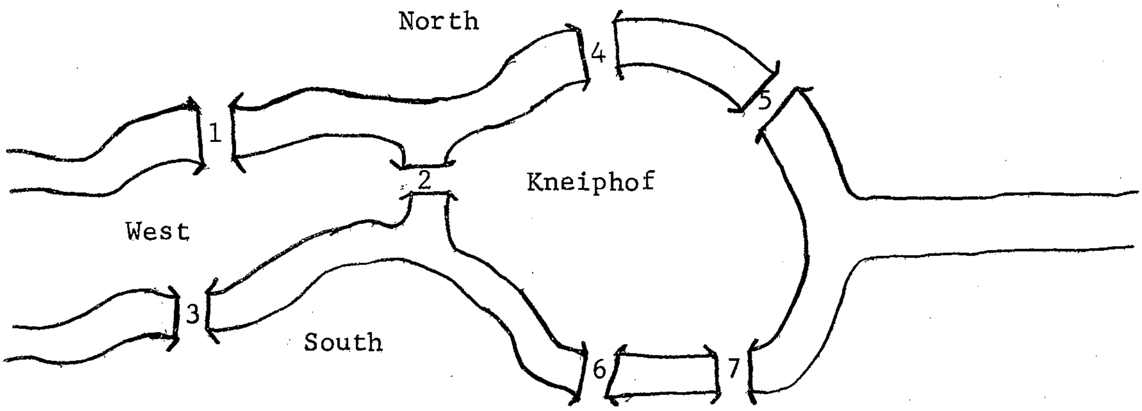


Figure 69

The problem simply stated is as follows: Is it possible to plan a walk in such a manner that, starting from any given position, one can return to that position after having crossed each river bridge just once?

It was Euler's fundamental analysis of this problem that lead to the study of graphs and ultimately gave rise to the science of combinatorial topology. Barnard attributes Euler's astonishing success as a mathematician to his genius for stripping away inessentials, and reducing the problem to its simplest form.[2]

In the case of the bridge problem, Euler imagined that the pieces of land had shrunk to mere points connected by lines representing the brides. Thus, Euler reduced the problem as given in Figure 69 to the diagram given in Figure 70.

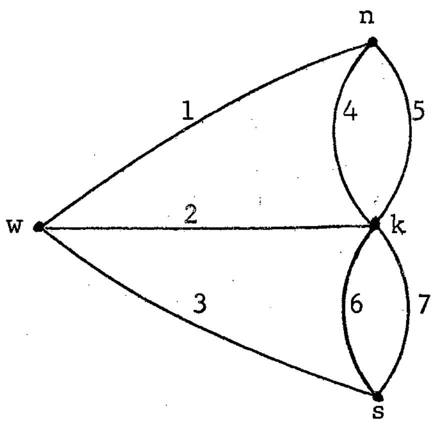


Figure 70

Euler then noted that if he could find a way to trace the whole figure without lifting his pencil from the paper, and without going over the same line twice, the Königsberg problem could be solved. Euler called such a path a unicursal route.

Euler concluded that this problem was not solvable and his reasoning was quite interesting. He called the points n, s, w, and k representing the land masses "nodes" and classified them as "odd-nodes" according to the number of lines joining at a particular point. Euler then made two rather remarkable observations concerning the traceability of a linear graph.

> (1) If there are no odd-nodes, then it is possible to start at any point and finish at that point.
> (2) If there are only two odd-nodes, then it is possible to start from one odd-node and finish at the other odd-node.[3]

Looking now at the bridge problem illustrated in Figure 70, it is easy to see that there are four nodes each of which is odd. Thus, the figure cannot be traced (or a unicursal path does not exist). The graph theory that developed from this simple beginning will be considered later. First, it seems appropriate to look briefly at the remarkability of Euler's observations.

Barnard points out that at the time that Euler was pondering over the Königsberg Bridge Problem, geometry was confined to the description of certain Euclidean figures such as squares, triangles, circles, etc. The theorems of Euclidean geometry established certain relationships that were true for plane Euclidean figures; however, if a triangle was irregularly shaped the normal Euclidean theorems did not apply. Thus, some mathematicians began to investigate the properties of geometric figures without concern for size and measurement. Their concern was mainly with the spatial relationships existing between a figure and its parts. For example, notice that there is little resemblance between the map in Figure 69 and the diagram in Figure 70. Barnard credits the recognition by Euler of the non-measurable properties of a figure as the spark that gave rise to the science of combinatorial topology.[4]

In mathematics, graph theory is classified as a branch of topology. The theory of graphs has applications in many diverse fields: electrical circuitry, programming, economics and psychology, to name just a few. Puzzles similar to the bridge problem have remained an intriguing part of the theory of graphs.

A linear graph is normally thought of as a certain collection of points called vertices and certain line segments connecting these vertices, called edges of the graph. To be somewhat more precise about what is meant by a graph, a graph will be defined abstractly as a representation of a set and a binary relation on that set.

<u>Definition 5.1</u>. The Cartesian cross-product of two sets A and B, denoted A X B, is the set of all ordered pairs in which a is in A and b is in B, that is,

$$A \text{ X } B = \{ (a, b) \mid a \in A \text{ and } b \in B \}.$$

For example, if $A = \{x, y\}$ and $B = \{1, 2\}$, then

$$A \text{ X } B = \{ (x,1), (x,2), (y,1), (y,2) \}.$$

<u>Definition 5.2</u>. A binary relation between two sets A and B is a subset of the ordered pairs in the carestian product A X B.

For example, $\{(a,x), (a,y), (b,y)\}$ is a binary relation between the sets $\{a,b,c\}$ and $\{x,y\}$. A binary relation between two sets can be represented in the form of a matrix or an array. For example, Figure 71 shows a representation of the relation {(a,x), (a,x), (b,y), (c,z)} between the sets {a,b,c} and {x,y,z}.

	x	y	z
a	✓		✓
b		✓	
c			✓

Figure 71

A check mark in a cell indicates that the element identifying the row that contains the cell and the element identifying the column that contains the cell are related. Notice that the row entry is the first position in the ordered pair, while the column entry is in the second position.

Definition 5.3. A binary relation on a set S is a binary relation between the set S and itself.

Thus, if R is a binary relation on S, the $R \subset S \times S$. For example, {(x,x), (x,y), (y,z), (z,x)} is a binary relation on the set {x,y,z}.

Definition 5.4. A binary relation R on a set S is called an equivalence relation if the following conditions are satisfied:

(1) Every element in the set S is related to itself, that is, for every $a \in A$, $(a,a) \in R$ or a R a (read a is related to a) (Reflexive Property)

(2) For any two elements a and b in S, if a is related to b, then b is also related to a, that is, if (a,b) $\in$ R, then (b,a) $\in$ R. (Symmetric Property)

(3) For any three elements a, b, and c in S, if a is related to b and b is related to c, then a is also related to c, that is, if (a,b) $\in$ R and (b,c) $\in$ R, then (a,c) $\in$ R. (Transitive Property)

There are many familiar equivalence relations that play an important role in the development of many areas of mathematics. For example, the following common equivalence relations: the equality relation "=" in various number systems, the congruence relation "≅" in geometry, and the congruence relation, "≡", in the integers.

In graph theory, the sets under consideration are normally quite small so it is feasible to represent a binary relation on a given set in matrix form. Consider the binary relations defined on the set $\{a,b,c,d\}$ as illustrated in Figure 72.

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

(a)

relation R_1

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

(b)

relation R_2

Figure 72

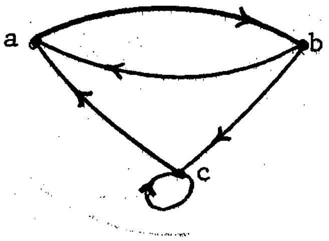
The binary relation illustrated in Figure 72(a) is an equivalence relation. Note that to check the reflexive property all one has to do is make sure the major diagonal is filled. The symmetry property can be checked by noting the symmetry about the major diagonal. Transitivity can be checked by inspecting the various possiblities. For example in Figure 72a, (a,b), (b,d) $\in R_1$ which implies that (a,d) must belong to R_1 if R_1 satisfies the transitive property.

In Figure 72(b), it should be obvious that R_2 is not symmetric and not transitive. However, R_2 is reflexive. For a more detailed discussion of relations see Eves and Newsom[5] or Ore[6].

The concept of a binary relation is now used to define what is meant by a linear graph. Let S = {a,b,c} and R be a binary relation defined by R = {(a,b), (b,a), (b,c), (c,a), (c,c)}. Figure 73(a) shows R represented in matrix form. An alternate way of representing the binary relation is shown in Figure 73(b).

	a	b	c
a		✓	
b	✓		✓
c			✓

(a)



(b)

Figure 73

The elements in S are represented by the points a, b, and c. The ordered pair (a,b) is represented by an arrow from a to b, and so on. Such a representation of a set and a binary relation defined on the set is called a linear graph.

Definition 5.5. A graph G is an ordered pair (S, R), where S is a set and R is a binary relation on S.

The elements of S are called vertices, and the ordered pairs in R are called edges of the graph. An edge (a,b) is said to be incident with the vertices a and b. For the graph G = (S, R) shown in Figure 74(a) there is a pair of edges joining every two vertices that are related, since R is a symmetric relation. Thus, R can be represented in Figure 74(b) where each edge represents two edges in Figure 74(a) and the direction arrows are omitted.

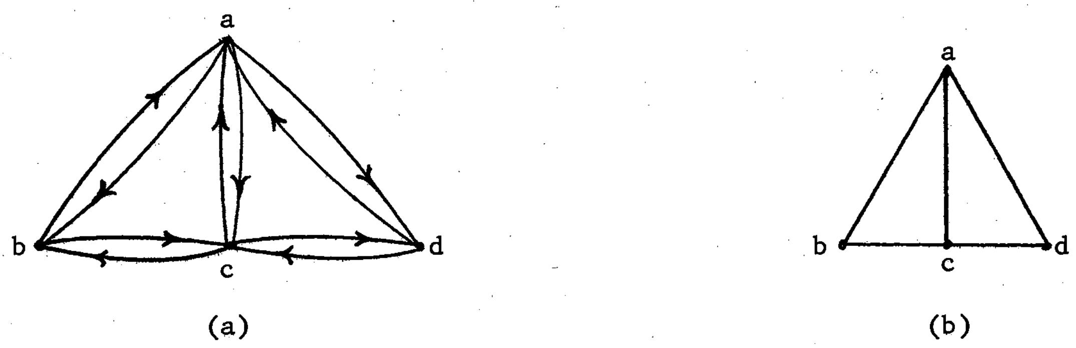


Figure 74

A graph is said to be a directed graph if directions are assigned to the edges and undirected if directions are not assigned to the edges. Thus, a set and a symmetric relation can be represented as a directed or undirected graph, but a set and a non-symmetric relation can only be represented by a directed graph.

To illustrate the concept of a graph somewhat more concretely, suppose that there are five different factories in the local area that exchange the parts that they produce. Denote the five factories by a, b, c, d, and e and let S = {a,b,c,d,e}. Let R be the binary relation "exchanges parts with." Suppose the general situation is as follows:

a exchanges parts with c and d

b exchanges parts with c, e, and d

c exchanges parts with a and b

d exchanges parts with a, e, and b

e exchanges parts with b and d.

This situation can be represented by a directed and undirected graph as illustrated in Figure 75.

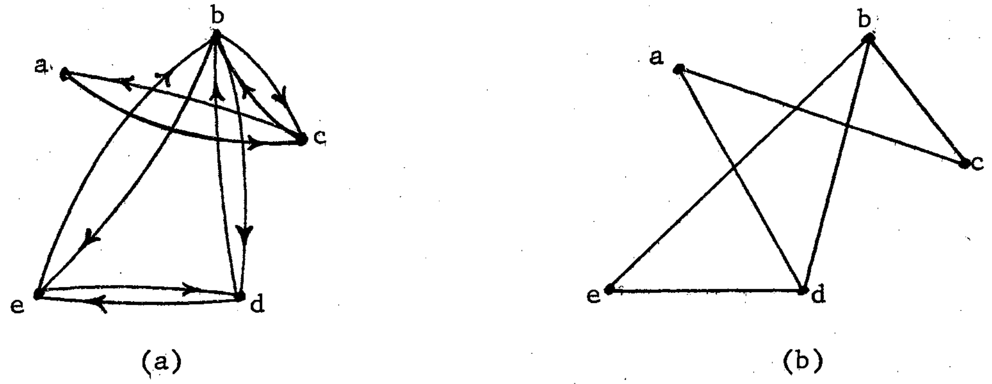


Figure 75

Notice that the edges of the graph appear to intersect although no new vertices are formed. One might think of the edges as threads crossing each other. The straight line segments of the undirected graph cause the most difficulty because of the resemblance to lines in Euclidean plane geometry. However, there is nothing that requires that the edges of an undirected graph be line segments so that Figure 75(a) could be represented as shown in Figure 76.

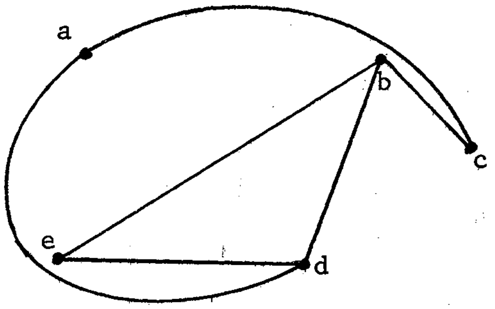


Figure 76

It is possible to have a null graph, that is, a graph which consists of isolated vertices with no edges. The graphs illustrated in Figure 77 are null graphs.

Definition 5.6. Two graphs are said to be isomorphic iff there is a one-to-one correspondence between their vertices and between their edges such that incidences are preserved.

Figure 77

Thus, if two graphs G_1 and G_2 are isomorphic, then if there is an edge between two vertices in G_1, there is a corresponding edge between the corresponding vertices in G_2. In the isomorphic graphs in Figure 78, the corresponding vertices are labeled with the same letters, primed and unprimed. To check the isomorphism simply check the incidence relations.

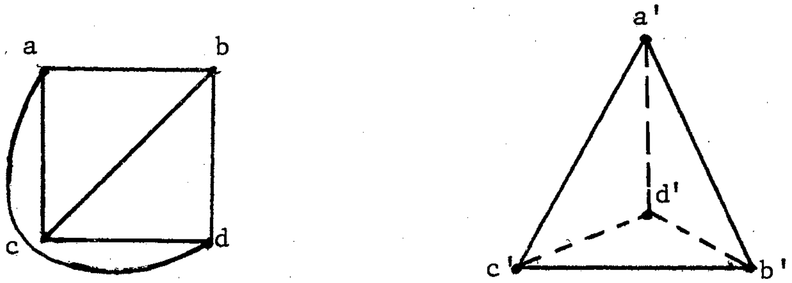


Figure 78

In a directed or undirected graph, the local degree of vertex is the number of edges that are incident with it. In a directed graph, the incoming degree of a vertex a is the number of edges that are incident to a, denoted by p(a), and the outgoing degree at a vertex a is the number of edges that are incident from a, denoted by p'(a). Thus, in a directed graph G with n vertices, v_1, v_2, . . ., v_n, the number of edges of G is given by

$N = p(v_1) + p(v_2) + . . . + p(v_n) = p'(v_1) + p'(v_2) + . . . + p'(v_n)$.

Figure 79 provides a simple example where p(v) and p'(v) = 1 for every vertex v of the graph.

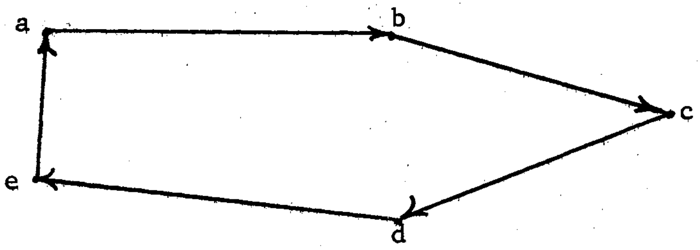


Figure 79

In the undirected graph in Figure 76, p(a) = p(c) = p(e) = 2 and p(b) = p(d) = 3.

It is often quite important to know the number of edges in a graph. One can always count the edges, but in general it is much easier to count the number of edges at each vertex and add. However, this process counts each edge twice so that the number of edges is half this sum. In general if G is a graph with n vertices, v_1, v_2, . . ., v_n, having local degrees $p(v_1)$, $p(v_2)$, . . ., $p(v_n)$, then the number of edges in G is

$$N = 1/2(p(v_1) + p(v_2) + . . . + p(v_n)).$$

Theorem 5.1. In any graph G, the sum of the local degrees is an even number.

Proof: The proof of this theorem follows directly from the fact that the number of edges in a graph G is $N = 1/2 \sum_{i=1}^{n} p(v_i)$. Thus, $\sum_{i=1}^{n} p(v_i) = 2N$ and the sum of the local degrees is an even number.

The vertices of a graph are classified as even or odd according to the number of edges incident at a particular vertex. For example in Figure 76 vertices a, c, and e are even while vertices b and d are odd.

Theorem 5.2. In any graph, there is an even number of odd vertices.

Proof: Let N be the number of edges in the graph. Then, since every edge contains two vertices, there are 2N vertices. Let V_1 be the number of vertices with only one incident edge, V_2 be the number of vertices with 2 incident edges, V_3 be the number of vertices with 3 incident edges, and so forth. Then it is required that $V = V_1 + V_2 + V_3 + \ldots$ is an even number. The number of vertices in the graph is $M = V_1 + 2V_2 + 3V_3 + 4V_4 + \ldots$ and $M = 2N$ which implies that M is an even number. Let $E = 2V_2 + 2V_3 + 4V_4 + 4V_5 + 6V_6 + 6V_7 \ldots$ and note that E is an even number. Therefore, $M - E = V_o$, where V_o is the number of odd vertices. But since the difference of two even numbers is even, V_o is even and the theorem is proven.

It is often useful to think of a graph as a road map where the edges correspond to roads and the vertices correspond to towns. For a given graph G, if it is possible to begin at some vertex a and follow a route that leads to k in any manner, then a is said to be connected to k. A route in G that passes no vertex twice is called an arc. The route in Figure 80 is an arc and c is connected to w.

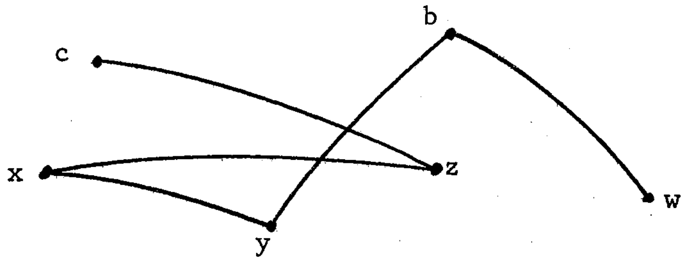


Figure 80

If every vertex in a graph is connected to every other vertex by an arc, then the graph is said to be connected. A route that never passes over the same edge twice is called a path. Notice that a path may pass the same vertex several times. If a path returns to the starting point, then it is referred to as a cyclic path or a circuit. In Figure 81, the route described by the sequence aecdb is an arc. The route described by the sequence aecdbe is a path and aedbeca is a circuit.

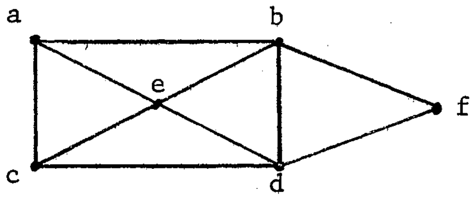


Figure 81

In certain graphs it is possible to find a cyclic path that passes through all edges just once. This is the type of path that Euler was concerned with in the Königsberg Bridge Problem. Thus, a cyclic path that passes through all edges just once is called an Euler path. Likewise, a circuit that passes through all edges just once is an Euler circuit.

The next theorem is adapted from theorems given by Busacher and Saaty.[7]

Theorem 5.3. An undirected graph possesses an Euler path iff it is connected and has no, or exactly two, vertices that are of odd local degree.

Proof: Suppose that a graph G possesses an Euler path L. Since G possesses an Euler path, G must be connected. When L is traced and the path meets a vertex, there are two edges that are incident with this vertex that have not been traced before since with the exception of the two terminal vertices of the path, the degree of any other vertex in the graph must be even. If the two terminal vertices of L are distinct, then their degrees must be odd. If the two terminal vertices coincide, then their degrees are both even, and L is an Euler circuit. Thus, the necessity of the condition is proven.

To prove the sufficiency of the condition, suppose that an Euler path L is constructed by starting at a, one of the two vertices of odd degree, and going through the edges of the graph G in such a way that no edge will be traced more than once. For a vertex of even degree, whenever the path enters the vertex through an edge, it can always leave the vertex through another edge that has not been traced before.

Thus, if G has no odd vertices, L must return to the vertex from which it started. If G has exactly two odd vertices, then L must end at the other odd vertex. If L passed through all edges, then L is an Euler path. If there is some vertex b such that L did not pass through b, then there are edges not traced by L. Therefore, b and all other vertices that were concurrent with L must have an even local degree. Define a second Euler path K similar to L beginning at b using the edges not contained in L. The path K must be cyclic since b has an even degree. Now, consider the path $L \cup K$. If $L \cup K$ is not an Euler path, then there must exist vertices in G not contained in $L \cup K$. In a similar manner, define a third path M and continue the process. Eventually by exhaustion, the graph G must contain an Euler path.

<u>Corallary 5.3.1</u>. A directed graph possesses an Euler circuit iff it is connected and its vertices are all of even degree.

<u>Corallary 5.3.2</u>. A directed graph possesses an Euler path iff it is connected and the incoming degree of every vertex is equal to its outgoing degree with the possible exception of two vertices. For these two vertices, the incoming degree of one is 1 larger than its outgoing degree, and the incoming degree of the other is 1 less than its outgoing degree.

<u>Corallary 5.3.3</u>. A directed graph possesses an Euler Circuit iff it is connected and the incoming degree of every vertex is equal to its outgoing degree.

Using Theorem 5.3, it is possible to solve many of the simpler puzzles that are associated with graph theory. Theorem 5.3 actually characterizes Euler's original observations. It is easy to see why the Königsberg Bridge Problem was not solvable since the graph representing the problem in Figure 70 has four odd vertices. Consider each of the undirected graphs illustrated in Figure 82.

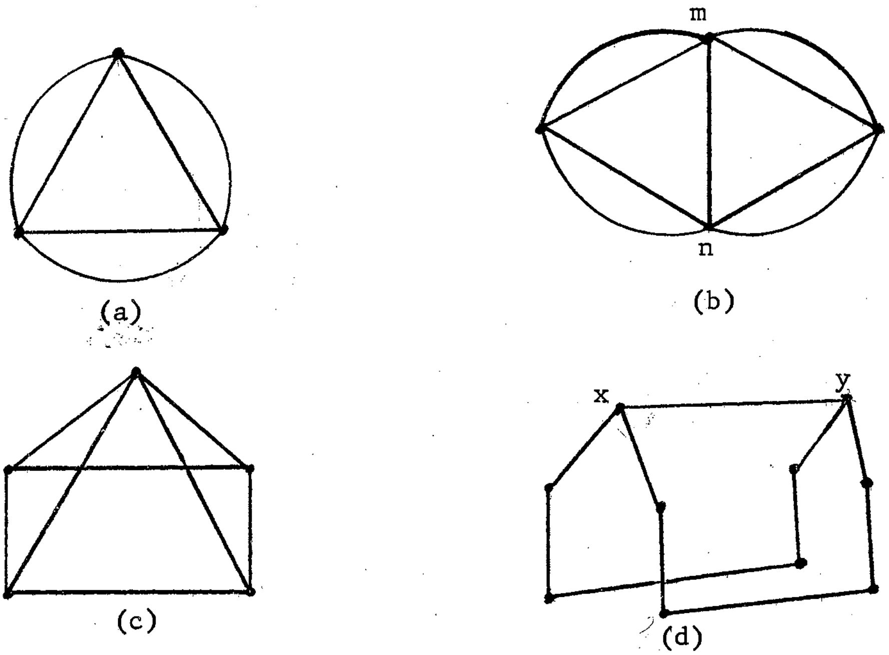


Figure 82

The graph illustrated in Figure 82(a) has an Euler path since there are four even vertices. In fact, an Euler circuit could begin at any of the vertices. Likewise, the graph illustrated in Figure 82(b) has an Euler path that must begin at either m or n. The graph in Figure 82(c) does not have an Euler path since there are four odd vertices. The graph in Figure 82(d) has an Euler path that could start at x or y.

The directed graph shown in Figure 83(a) does not have an Euler path by Corallary 5.3.2. However, the graph illustrated in Figure 83(b) does have an Euler path.

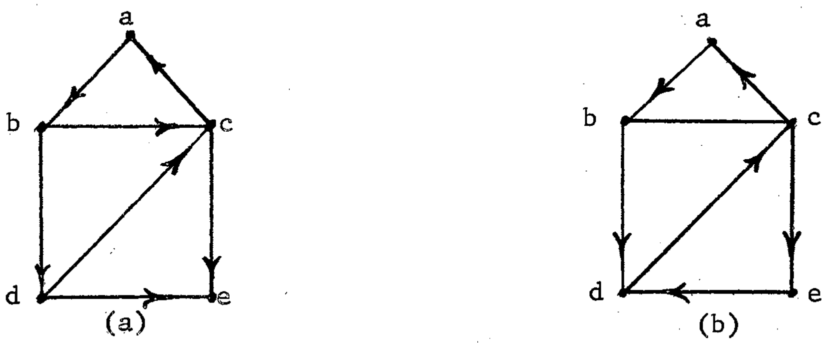


Figure 83

A classic puzzle involving the basic concept of an Euler path is the Sixteen Door Problem. To illustrate this problem, consider the five roomed house with sixteen doors arranged as shown in Figure 84.

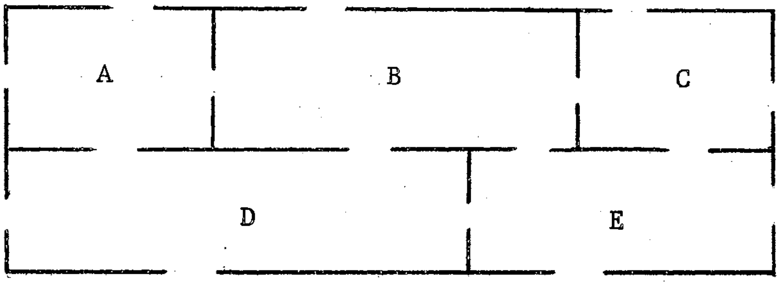


Figure 84

The problem asks whether it is possible to draw a continuous line without lifting the pencil from the paper, passing through each door once and only once. The solution to the problem is not difficult using graph theory, but one might spend a considerable amount of time attempting to solve the problem by trial and error. To solve the problem, simply note that rooms B, D, and E have five doors each. Thus, the number of vertices with odd local degrees would be three. Hence, the problem is not solvable.

There is another problem that often arises which is similar to the question of whether or not a particular graph has an Euler path. The most familiar example of a problem of this type was posed by an Irish mathematician Sir William Row Hamilton.[8] Hamilton developed a puzzle by using a polyhedron having regular pentagons for its faces, with three edges of these pentagons meeting at each of the 20 corners. Hamilton labelled each corner with the name of an important city. The problem consisted of finding a route along the edges of the dodecahedron which passed through each city exactly once. The dodecahedron was a rather cumbersome figure to work with so Hamilton revised the problem by constructing a plane figure which was isomorphic to the dodecahedron. The cross shaded route shown in Figure 85 is a solution to the problem.

In honor of Hamilton's Travelers Dodecahedron Problem, a path in a graph that passes through each vertex exactly once is called a Hamilton path. It is interesting to note that mathematicians have found no criteria for the existence of a Hamilton path in a graph.

Ore suggests that many of the problems in the field of operations research are very similar to the problem of finding a Hamilton path. For example, a traveling salesman wants to visit a number of cities on a particular route. The salesman is interested in finding a route that is the most economical in terms of time and money. A problem of this type can be solved by trial and error, but this is often very costly.[9]

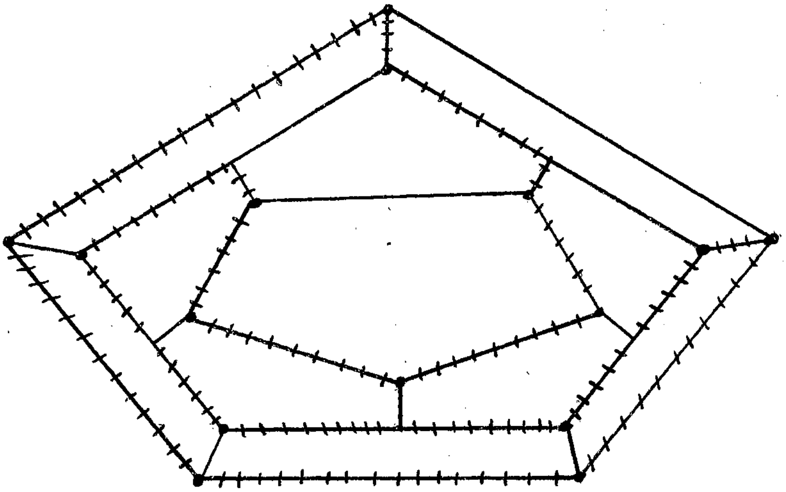


Figure 85

Many problems in graph theory depending on the existence or non-existence of Hamilton paths cannot be solved. This points out one of the intriguing aspects of mathematics. A rather interesting approach to problems involving Euler and Hamilton paths is given by S. K. Stein.[10]

FOOTNOTES

[1] Oystein Ore, Graphs and Their Uses (New York, 1963), p. 23.

[2] D. S. Banard, Adventures in Mathematics (New York, 1967), p. 67.

[3] Ibid., p. 68.

[4] Ibid., p. 71.

[5] H. Eves and C. V. Newsom, An Introduction to the Foundations and Fundamental Concepts of Mathematics (New York, 1965), pp. 148-153.

[6] Ore, pp. 80-93.

[7] R. G. Busacker and T. L. Saaty, Finite Graphs and Networks: An Introduction with Applications (New York, 1965), pp. 13-32.

[8] Ore, p. 28.

[9] Ibid., p. 30.

[10] S. K. Stein, Mathematics: The Man-Made Universe (San Francisco, 1963), pp. 95-110.

CHAPTER VII

A SET THEORETIC APPROACH TO FINITE PROBABILITY

The word "probability" means many things to many people. For example, one often hears phrases such as "the probability of fair weather over the weekend," or "the probability of the Mets winning the world series." In each of these cases, the word probability has only a vague meaning. However, the development of a mathematical theory of probability depends on a precise definition of "probability." Before a formal discussion of the theory of probability is introduced, it might be interesting to note the origins of probability theory and some of its applications.

The founders of the mathematical theory of probability were two French mathematicians of the seventeenth century, Pierre Fermat (1601-1665) and Blaise Pascal (1623-1662). Both of these men are well known for their contributions to mathematics. Fermat is most noted for his discoveries in the theory of numbers, and Pascal for his work in geometry. Historically, the initial problem out of which evolved the theory of probability was a gambling problem proposed by a gambler, the Chevalier de Méré. The problem was basically a question of how the stakes should be divided between two players in a game of chance if the game was stopped before the game was finished. In the course of solving this rather simple problem, other challenging questions in probability and laws of chance occurred to Pascal. Unable to solve them, he turned to his friend Fermat, and a very profitable correspondence arose which, in time, resulted in some of the basic concepts of the theory of probability.[1]

The theory that originated in a game of chance has become of great importance in the modern world. It is the mathematical foundation of numerous kinds of financial insurance and mathematical statistics. It finds applications in many aspects of the biological and social sciences, physics, and engineering.

In the discussion that follows, illustrations using dice, cards, or coins will be used since these objects are familiar and their probabilistic aspects are often reasonable to compute. Moreover, they provide good illustrations of the basic principles of the theory.

Probability is commonly referred to as the mathematics of chance. Frequently, one wishes to determine how likely it is that a certain event will occur. One obvious approach to the problem is to perform an experiment under controlled conditions and observe the outcomes.

Definition 7.1. An experiment is any operation whose outcome cannot be predicted with certainty.

Definition 7.2. The sample space of an experiment is the set of all possible outcomes for the experiment.

Example 7.1. Consider the experiment of rolling a single die one time. The sample space for this experiment is $S_1 = \{1,2,3,4,5,6\}$ where the integers 1 through 6 represent the number of spots on the upmost face of the die after it stops rolling. For the same experiment, another sample space is $S_2 = \{\text{even, odd}\}$ where the list of possible outcomes is even and odd numbered faces of the die.

Example 7.2. Consider the experiment of tossing a coin. The sample space is $S_1 = \{H, T\}$ where H denotes a head and T denotes a tail. If two coins were tossed, then the sample space would be

$$S_2 = \{HH, HT, TH, TT\}.$$

Example 7.3. Consider the experiment of rolling a pair of dice, one red and the other green. The sample space consists of the 36 outcomes listed in S. The first position represents the number corresponding to the red die and the second corresponds to the green die.

$$S = \left\{\begin{array}{cccccc} (1,6) & (2,6) & (3,6) & (4,6) & (5,6) & (6,6) \\ (1,5) & (2,5) & (3,5) & (4,5) & (5,5) & (6,5) \\ (1,4) & (2,4) & (3,4) & (4,4) & (5,4) & (6,4) \\ (1,3) & (2,3) & (3,3) & (4,3) & (5,3) & (6,3) \\ (1,2) & (2,2) & (3,2) & (4,2) & (5,2) & (6,2) \\ (1,1) & (2,1) & (3,1) & (4,1) & (5,1) & (6,1) \end{array}\right\}$$

Definition 7.3. An event is a subset of the sample space. Every subset of the sample space is an event.

In Example 7.2 where the sample space was $S = \{H,T\}$, the sets $A = \{H,T\}$, $B = \{H\}$, and $C = \{T\}$ are events. Likewise, in Example 7.1, the sets $A = \{1,3,5\}$, $B = \{2,4,6\}$, and $C = \{1,2\}$ are events.

The theory of probability is concerned with establishing a consistent way of assigning numbers to events which are called probabilities of the occurrence of these events. Thus, probability can be thought of as a measure applied to the events that can occur in a given experiment. Formally, the probability measures must satisfy the three axioms given in Definition 7.5 defined in terms of a probability function.

Definition 7.4. A rule f which associates a real number with each subset of some universal set is called a real-valued set function.

For example, if $S = \{a,b,c\}$, then the possible subsets of S are $\{ \phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\} \}$. Then a rule f defined by $f(A) = 0$ if $1 \in A$ and $f(A) = 1$ if $1 \notin A$, where $A \subset S$, is a set function.

Definition 7.5. A probability function is a real-valued set function defined on the class of all subsets of the sample space S satisfying the following three axioms:[2]

(1) $P(S) = 1$ (Axiom 1)

(2) $P(A) \geq 0$ for all $A \subset S$ (Axiom 2)

(3) $P(A_1 \cup A_2 \ . \ . \ . \cup A_n) = P(A_1) + P(A_2) + \ . \ . \ . + P(A_n)$

if $A_i \cap A_j = \phi$ for all $i \neq j$. (Axiom 3)

Example 7.4. Consider the experiment in which a fair die is rolled once, as in Example 7.1. The sample space is $S = \{1,2,3,4,5,6\}$. Since the die is fair, the outcomes are equally to occur, so it would seem reasonable to assume that each outcome should be assigned the same probability. Let $E_1 = \{1\}$, $E_2 = \{2\}$, $E_3 = \{3\}$, $E_4 = \{4\}$, $E_5 = \{5\}$, and $E_6 = \{6\}$. Axiom 1 implies that $P(S) = 1$ and Axiom 3 implies that $P(E_1 \cup E_2 \ . \ . \ . \cup E_6) = P(E_1 + P(E_2) + \ . \ . \ . + P(E_6)$ since $E_i \cap E_j = \phi$ if $i \neq j$. But $\sum_{i=1}^{6} P(E_i) = P(S)$, therefore, $P(E_1) + P(E_2) + \ . \ . \ . + P(E_6) = 1$ and each event is equally likely. Let $P(E_i) = 1/6$, $i = 1,2,3,4,5,6$.

Example 7.5. Consider the experiment of tossing a biased coin. Suppose that based on a statistical study of a particular coin, it is known that a tail is twice as likely to occur as a head. What probability measure should be assigned to each outcome? Let $S = \{H,T\}$, $A = \{H\}$, and $B = \{T\}$. If the $P(A) = x$, then $P(B)$ should be $2x$ since a tail is twice as likely to come up as a head. But by Axiom 3, $P(A \cup B) = P(A) + P(B)$ since $A \cap B = \phi$. Axiom 1 implies that $P(S) = P(A \cup B) = 1$. Thus, $P(A) + P(B) = x + 2x = 1$ or $x = 1/3$. Therefore, let $P(A) = 1/3$ and $P(B) = 2/3$.

Definition 7.6. If E is an event, then E' denotes the complement of E relative to S. E' is called the complementary event of E.

The following sequence of theorems was adapted from theorems and problems in Parzen.[3]

Theorem 7.1. If E is an event in a sample space S, then $P(E) + P(E')$ $= 1$.

Proof: It is evident that $E \cup E' = S$, while $E \cap E' = \phi$. Thus, by Axiom 3 $P(E \cup E') = P(E) + P(E')$. But $P(E \cup E') = P(S) = 1$ by Axiom 1. Therefore, $P(E) + P(E') = 1$.

Theorem 7.2. $P(\phi) = 0$ for any sample space S.

Proof: First, note that $S \cup \phi = S$. Thus, $P(S \cup \phi) = P(S) = 1$ by Axiom 1. But $S \cap \phi = \phi$ so that $P(S \cup \phi) = P(S) + P(\phi) = 1 + P(\phi)$ by Axiom 3. Thus, $1 + P(\phi) = 1$ which implies that $P(\phi) = 0$.

Example 7.6. Given $S = \{1,2,3\}$, $A = \{1,2\}$, $B = \{3\}$, $C = \{2\}$, $P(A) = 2/3$, and $P(B) = 1/3$. Find $P(A \cap B)$ and $P(A \cap C)$. Since $A \cap B = \phi$, then $P(A \cap B) = P(\phi) = 0$. But $(A \cap C) = \{2\}$ so $P(A \cap C) = P(\{2\}) = P(C)$. Theorem 7.1 implies that $P(C) + P(C') = 1$ which implies $P(C) = 0$. Therefore $P(A \cap C) = 0$.

Theorem 7.3. If A and B are events of a sample space S, then

$$P(A' \cap B) = P(B) - P(A \cap B).$$

Proof: B can be written as $B \cap S$, but $A \cup A' = S$. Thus,

$$B = B \cap S = B \cap (A \cup A') = (B \cap A) \cup (B \cap A')$$

since $\cap$ distributes over $\cup$. Then $P(B) = P(\ (B \cap A) \cup (B \cap A')\ )$. But since $(B \cap A) \cap (B \cap A') = \phi$, Axiom 3 implies that

$$P(B) = P(B \cap A) + P(B \cap A').$$

Thus, $P(A' \cap B) = P(B) = P(A \cap B)$.

Theorem 7.4. If A and B are events in a sample space S, then

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Proof: First, note that $A \cup B = S \cap (A \cup B) = (A \cup A') \cap (A \cup B) = A \cup (A' \cap B)$ since $\cup$ distributes over $\cap$. Thus, $P(A \cup B) = P(A \cup (A' \cap B))$. But $A \cap (A' \cap B) = \phi$, therefore, by Axiom 3 $P(A \cup (A' \cap B)) = P(A) + P(A' \cap B)$. But $P(A' \cap B) = P(B) - P(A \cap B)$ by Theorem 7.3 which implies that

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Example 7.7. Suppose that $S = \{1,2,3\}$, $A = \{1\}$, $B = \{2\}$, and $C = \{3\}$. Suppose also that an experiment is run so that $P(A) = 1/2$ and $P(B) = 1/5$. Compute the probabilities: (a) $P(C)$, (b) $P(A \cup B)$, (c) $P(A')$, and (d) $P(A' \cap B')$.

(a) First, note that $A \cup B \cup C = S$. Thus, $P(A \cup B \cup C) = P(A) + P(B) + P(C) = 1/2 + 1/5 + P(C) = 1$ which implies that $P(C) = 3/10$.

(b) By Theorem 7.4, $P(A \cup B) = P(A) + P(B) - P(A \cap B)$. But $A \cap B = \emptyset$, therefore by Theorem 7.2 $P(A \cap B) = 0$. Thus, $P(A \cup B) = P(A) + P(B) = 1/2 + 1/5 = 7/10$.

(c) $P(A) + P(A') = 1$ by Theorem 7.1. Thus, $P(A') = 1 - P(A) = 1/2$.

(d) $P(A' \cap B') = P(B') - P(A \cap B')$ by Theorem 7.3. $P(B') = 1 - P(B) = 1 - 1/5 = 4/5$ by Theorem 7.1. $B' = \{1,3\}$ and $A = \{1\}$ which implies that $A \cap B' = \{1\} = A$. So $P(A \cap B') = P(A) = 1/2$. Thus, $P(A' \cap B') = P(B') - P(A \cap B') = 4/5 - 1/2 = 3/10$.

When dealing with finite sample spaces, it is quite convenient to assign probability to a given event A by considering the probabilities of the single element events that comprise A.

__Definition 7.7__. A single-element event is a subset of the sample space S which contains one and only one element of S.

Thus, if $S = \{1,2,3\}$, then the single element events are $\{1\}$, $\{2\}$, and $\{3\}$. For the sample space {HH, HT, TH, TT}, the single-element events are {HH}, {HT}, {TH}, and {TT}. Thus, if S has n elements, then there are exactly n distinct single-element events.

__Theorem 7.5__. Let S be any sample space and E S, then $P(E) = \sum_{k=1}^{n} P(E_i)$ where $E_1, E_2, E_3, \ldots, E_n$ are distinct single-element events and $E = E_1 \cup E_2 \cup E_3 \ldots \cup E_n$.

Proof: Since $E_1, E_2, \ldots, E_n$ are distinct single-elements events, $E_i \cap E_j = \emptyset$ for $i \neq j$. Axiom 3 implies that $P(E) = P(E_1 \cup E_2 \cup \ldots \cup E_n = P(E_1) + P(E_2) + \ldots + P(E_n) = \sum_{i=1}^{n} P(E_i)$.

For experiments in which it is reasonable to assume that each single element event is equally likely to occur, then it is quite easy to assign probabilities to the events when the sample space is finite.

Definition 7.8. If A is a set, then n(A) is the number of elements in A. n(A) is read "the number property of A."

The number property of a set can be used to assign probability to any event $A \subset S$ when the outcomes are equally likely. Suppose that there are n equally likely outcomes to an experiment. Since $P(S) = 1$ and each of the outcomes are equally likely, the probability assigned to a single-element event must be 1/n. Any event $E \subset S$ must be a union of single-element events; thus, P(E) can be written as the sum of the probabilities of the single-element events that comprise E. Hence, it would seem reasonable to let $P(E) = \frac{n(E)}{n(S)}$ where $E \subset S$. To see that this assignment of probability satisfies the three axioms for a probability function, the following theorem is proved.

Theorem 7.6. If S is a sample space with k elements and $E \subset S$, then the probability assignment given by $P(E) = \frac{n(E)}{n(S)}$ satisfies the three axioms for a probability function.

Proof: Since S has k elements, $n(S) = k$. Thus, $P(S) = \frac{n(S)}{n(S)} = \frac{k}{k} = 1$ so Axiom 1 is satisfied. If $E \subset S$, then $n(E) \geq 0$. Thus, $P(E) = \frac{n(E)}{n(S)} \geq 0$ for any $E \subset S$ and Axiom 2 is satisfied. If $E_1 \cap E_2 = \phi$, then $n(E_1 \cup E_2) = n(E_1) + n(E_2)$. Hence, if $E_1 \subset S$ and $E_2 \subset S$ with $E_1 \cap E_2 = \phi$, then

$P(E_1 \cup E_2 = \frac{n(E_1 \cup E_2)}{n(S)} = \frac{n(E_1)}{n(S)} + \frac{n(E_2)}{n(S)} = P(E_1) + P(E_2)$. A similar argument could be given for any number of subsets.

Example 7.8. Consider an experiment where a fair coin is tossed 3 times. The sample space could be illustrated by

$$S = \{ \text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT} \}.$$

Since $n(S) = 8$, the probability of 1/8 could be assigned to each single-element event. Let E_1 be the event that exactly two tails occur and let E_2 be the event that at least one tail occurs. Find $P(E_1)$ and $P(E_2)$. First, note $E_1 = \{\text{HTT, THT, TTH}\}$, so that $P(E_1) = \frac{n(E_1)}{n(S)} = 3/8$. Since $E_2 = \{\text{HHT, HTH, HTT, THH, THT, TTH, TTT}\}$, $P(E_2) = \frac{n(E_2)}{n(S)} = 7/8$. Often times it is easier to find the probability of the complement of an event and then use Theorem 7.1. For example, $E'_1 = 1/8$ and Theorem 7.1 implies that $P(E_1) = 1 - P(E'_1) = 1 - 1/8 - 7/8$.

Example 7.9. Consider an experiment of drawing a card from an ordinary deck of cards. Assume that each of the 52 cards is equally likely to be drawn. Let E_1 be the event that an ace is drawn, E_2 the event a spade is drawn, and E_3 the event that an ace of spades is drawn. Assume that the 52 cards are ordered in some manner and a unique number from 1 to 52 is assigned to each card. Then, $S = \{1, 2, 3, . . ., 52\}$. $n(E_1) = 4$ since there are 4 aces in an ordinary deck of cards. Thus, $P(E_1) = n(E_1)/n(S) = 4/52$. Similarly, $P(E_2) = n(E_2)/n(S) = 13/52$ and $P(E_3) = n(E_3)/n(S) = 1/52$.

Definition 7.9. An item is selected at random from a group of items if the selection procedure is such that each item in the group is equally likely to be selected.

Example 7.10. Let S be a set of 60 students studying at least one of two languages French or German. Let F represent the set of students studying French and G represent the set of students studying German. Assume the following information is known: $n(F) = 30$, $n(G) = 50$, and $n(F \cap G) = 20$. What is the probability that a student selected at random (1) will study German and French, (2) will study German but not French. The Venn diagram in Figure 86 will help illustrate the problem.

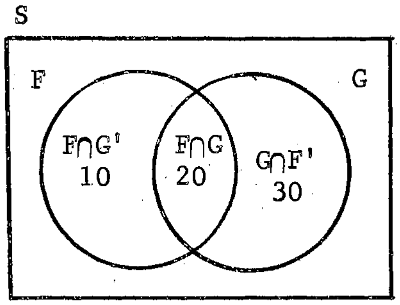


Figure 86

The solutions are:

(1) $P(F \cap G) = n(F \cap G)/n(S) = 20/60 = 1/3$

(2) $P(G \cap F') = n(G \cap F')/n(S) = 30/60 = 1/2$

Many of the solutions to probability problems depend on being able to count the elements belonging to particular sets. There are many useful techniques available. The two most common counting techniques involve permutations and combinations.

Definition 7.10. An arrangement of n symbols in definite order is called a permutation of n symbols.

Frequently, one is interested in selecting and arranging a specified number of elements of a set. For example, one may wish to select r elements from a set of n elements, where $r \leq n$, and then arrange these r elements in some order.

Definition 7.11. The number of different arrangements, each consisting of r elements, that can be selected from a set of n distinct elements is called the number of permutations of n elements taken r at a time, and is denoted by ${}_nP_r$.

Theorem 7.7. ${}_nP_r = n(n - 1)(n - 2) \ . \ . \ . \ (n - r+1)$.

To see that this theorem is valid, simply note that the first of the r positions in a permutation can be filled in n different ways. Then the second position can be filled in n - 1 different ways, the third in n - 2 ways, and so on. Thus, the number of ways of filling each position is n minus the number of positions already filled. When the rth element is to be chosen, r-1 places have already been filled. Hence, the rth position can be filled in $n -(r - 1) = n - r + 1$ ways.

Definition 7.9. $k! = k(k - 1)(k - 2) \ . \ . \ . \ 3.2.1$ for integers $k \geq 0$ and $0! = 1$.

Theorem 7.8. ${}_nP_r = n!/(n - r)$.

Proof: ${}_nP_r = n(n - 1) \ . \ . \ . \ (n - r + 1)$ from Theorem 7.7. Then, note that multiplying ${}_nP_r$ by $(n - r)!/(n - r)!$ does not change the value of ${}_nP_r$. Thus,

$$\begin{aligned} {}_nP_r &= n(n - 1)(n - 2) \ . \ . \ . (n - r + 1). \ (n - r)! \ /(n - r)! \\ &= \frac{n(n - 1)(n - 2) \ . \ . \ . \ (n - r + 1)(n - r)(n - r - 1) \ ... \ 2.1}{(n - r)!} \\ &= \frac{n!}{(n - r)!} \end{aligned}$$

<u>Example 7.11</u>. How many permutations can be formed from the letters of the word BACKSPIN if four letters are taken at a time? The answer is ${}_8P_4 = 8!/4! = 8.7.6.5 = 1680$.

<u>Definition 7.10</u>. The number of subsets, each of size r, that a set with n elements has is called the number of combinations of n things r at a time and is denoted by ${}_nC_r$.

If A is a set of n elements, note that ${}_nP_r$ counts the number of different arrangements of subsets containing r elements. However, ${}_nC_r$ counts the number of different subsets of A, each containing r elements. But since sets are not ordered, there are ${}_rP_r$ different arrangements of the ${}_nC_r$ subsets, that is, ${}_nC_r \cdot {}_rP_r = {}_nC_r . r! = {}_nP_r$. But ${}_nP_r = n!/(n - r)!$ which implies that ${}_nC_r \ . \ r! = n!/(n - r)!$ or that ${}_nC_r = n!/r!(n - r)!$.

<u>Example 7.12</u>. If 10 boys go out for basketball at a particular school, then how many different teams could be fielded from these boys? The answer is ${}_{10}C_5 = 10!/5!5! = 252$.

The most difficult part of many counting problems is deciding whether ordering should be of importance. If order does not matter, use combinations; however, if order is important use permutations. A very interesting and quite refreshing approach to counting problems is given by Niven[4].

To help acquaint the reader with counting techniques and their applications to probability problems, the following example are provided.

Example 7.13. A bridge hand consists of a 13 card subset of the set of 52 cards in an ordinary deck of playing cards. Find the probability that a bridge hand chosen at random contains all four kings of the deck. Let E be the event of a hand containing four kings. Let S be the set of all possible bridge hands. Since each hand consists of 13 cards chosen at random from the 52 cards, $n(S) = {}_{52}C_{13}$. Since the cards are chosen at random, one hand is as likely as any other. Thus, $P(E) = n(E)/n(S)$. Since the deck only contains four kings, the four kings can be selected ${}_4C_4$ ways, while the other 9 cards can be selected from the remaining 48 cards in ${}_{48}C_9$ ways. Therefore, $P(E) = n(E)/n(S) = {}_4C_4 \cdot {}_{48}C_9/ {}_{52}C_{13} = 11/(17)(5)(49)$.

Example 7.14. Suppose a box contains 5 red and 4 white balls. Three balls are drawn at random. What is the probability of obtaining 3 red balls and obtaining 2 red balls and 1 white ball. Let E_1 be the event of drawing 3 red balls and E_2 be the event of drawing 2 red balls and 1 white ball. Let S be the possible outcomes when 3 balls are drawn. $n(S) = {}_9C_3 = 9!/3!\,6! = 84$. Since there are 5 red balls, the number of ways E_1 can happen is the number of ways 3 balls can be chosen from

5 or ${}_5C_3 = 10$. Since each ball is equally likely to be drawn, $P(E_1) = n(E_1)/n(S) = 10/84 = 5/42$. Similarly, $P(E_2) = n(E_2)/n(S)$. The number of ways in which 2 red balls can be picked from 5 red balls is ${}_5C_2 = 10$. The number of ways 1 white ball can be selected from 4 white balls is ${}_4C_1 = 4$. However, each of the ways of picking 2 red balls can happen simultaneously with each of the ways of picking 1 white ball. Thus, 2 red balls and 1 white ball can be selected in $10 \cdot 4$ or 40 ways which implies $n(E_2) = 40$. Therefore, $P(E_2) = n(E_2)/n(S) = 40/84 = 10/21$.

It is interesting to note that many problems involving probability do not appeal to one's intuition about a particular problem. Probably the most famous problem illustrating this is the so called Birthday Problem[5].

Example 7.15 (The Birthday Problem). Suppose that n people are in a room. What is the probability that at least two of the people have the same birthday? For the purposes of this problem, assume that there are only 365 days available for birthdays and that each of the days is equally likely to occur. The solution set of possible birthdays is A = {Jan. 1, Jan. 2, . . ., Dec. 30, Dec. 31}. For convenience, suppose the days are numbered from 1 to 365. Then A can be written, $A = \{1,2,3, \ldots, 365\}$. Suppose that n birthdays are expressed in an ordered n-tuple $(b_1, b_2, \ldots, b_n)$ where b_1 is the number representing the birthday of the first person; b_2 is the number representing the birthday of the second person, and so on. Then it is fairly obvious that the sample space is the collection of all possible n-tuples that could occur for the birthdays. Symbollically,

$S = \{(b_1, b_2, \ldots, b_n) \mid b_i \in A, i = 1,2, \ldots, n\}$. Since there are 365 choices for each birthday, there are 365^n possibilities for the birthdays of n people, that is, $n(S) = 365^n$.

Now define E to be the event that at least two people have the same birthday. Then E' is the event that no two people in the room have the same birthday. Since P(E') is easier to find, P(E') will be computed and then Theorem 7.1 will be used to find P(E).

Since $P(E') = n(E')/n(S) = N(E')/365^n$, the problem reduces to finding n(E'). Observe that n(E') is equivalent to the number of ways of selecting n different numbers from a set of 365 different numbers. Thus, $n(E') - {}_{365}P_n = 365 \cdot 364 \ldots (365-n+1)$. Therefore, $P(E') = 365 \cdot 364 \cdot \ldots (365 - n + 1)/ 365^n$ and by Theorem 7.1 $P(E) = 1 - P(E') = 1 - (365 \cdot 364 \cdot \ldots (365 - n + 1))/365^n$. If $n = 4$, then $P(E) = 1 - (365 \cdot 364 \cdot 363 \cdot 362)/365^4 \approx 1 - 0.984 \approx 0.016$. Thus, if four people selected at random were in a room, the probability of at least two people having the same birthday is 0.016. Using a similar process and letting n vary for values between 10 and 60, the values as shown in the table in Figure 87 could be derived.

Notice that if $n > 22$, then $P(E) > 1/2$ which is rather surprising. However, if $n = 60$, then $P(E) = .994$. Thus, in a random group of 60 people it is almost a certainty that at least two of the people have the same birthday. This is a very interesting conclusion and certainly does not appeal to one's intuition.

Often times the probability of events with certain conditions attached are needed. For example, suppose that an event E_1 has occurred and you are asked to find the probability of an event E_2 from the sample space. For a specific example consider the following situation: suppose a team of medical researchers are conducting an experiment. A randomly selected person is found to have a family history of diabetes. What is the probability that this person also has diabetes? Questions of this type lead to conditional probabilities.

n	P(E')	P(E)
10	.871	.129
20	.589	.411
21	.556	.444
22	.524	.476
23	.493	.507
30	.294	.706
40	.109	.891
50	.030	.970
60	.006	.994

Figure 87

Definition 7.12. The conditional probability of B occurring, given that A has occurred (written $P(B|A)$) is $P(B|A) = P(B \cap A)/P(A)$ if $P(A) > 0$. If $P(A) = 0$, then defined $P(B|A) = 0$.

Example 7.16. Suppose that two dice are thrown. What is the probability that the sum of the two faces is 7, knowing that one face has turned up 5? The sample space obviously contains 6^2 outcomes; however, only a subset of these 36 outcomes need be considered. Let A be the subset of S where at least one member is a 5. Thus, A = $\{(5,1), (5,2), (5,3), (5,4), (5,5), (5,6), (1,5), (2,5), (3,5), (4,5), (6,5)\}$ which implies that n(A) = 11. Let B be the event that the faces sum to 7. Then B = $\{(2,5), (5,2)\}$ and n(B) = 2. $P(B \cap A) = n(B \cap A)/n(S) = 2/36$ and $P(A) = n(A)/n(S) = 11/36$. Therefore, $P(B|A) = P(B \cap A)/P(A) = (2/36)/(11/36) = 2/11$.

Example 7.17. Given that 10 per cent of the light bulbs produced are blue and 2 per cent of all bulbs are blue and defective. What is the probability that a bulb selected at random is defective if it is known that it is blue?

Let A be the event that the light bulb is blue and B be the event that the light bulb is defective. Then, $P(B\ A)/P(A) = (2/100)/(10/100) = 1/5$.

One of the most useful results in problems involving conditional probability is known as Bayes' Theorem or Bayes' formula. Bayes' Theorem has recently been applied to many different kinds of problems. The proof of Bayes' Theorem is adopted from Larsen.[6]

Theorem 7.9 (Bayes). Suppose that k events $A_1, A_2, \ldots, A_k$ are given such that $A_1 \cup A_2 \cup \ldots \cup A_k = S$ and $A_i \cap A_j = \phi$ for all $i \neq j$; then for an event $E \subset S$,

$$P(A_j|E) = P(A_j)P(E|A_j) \Big/ \sum_{i=1}^{k} P(A_i)P(E|A_i), \quad j = 1,2,3, \ldots, k.$$

Proof: Since $A_1 \cup A_2 \cup \ldots \cup A_k = S$ and $A_i \cap A_j = \phi$ for $i \neq j$, then for any event $E \subset S$, $E = (E \cap A_1) \cup (E \cap A_2) \cup \ldots \cup (E \cap A_k)$. Since $(E \cap A_i) \cap (E \cap A_j) = \phi$ for $i \neq j$, then

$P(E) = P(E \cap A_1) + P(E \cap A_2) + \ldots + P(E \cap A_k)$. But $P(E \cap A_i) = P(A_i)P(E|A_i)$ for each i by Definition 7.11. Thus, $P(E) = P(A_1)P(E|A_1) + P(A_2)P(E|A_2) + \ldots + P(A_k)P(E|A_k)$. By definition, $P(A_j|E) = P(A_j \cap E)/P(E)$, $j = 1,2,3, \ldots, k$. Hence,

$$P(A_j|E) = P(A_j)P(E|A_j)/ \sum_{i=1}^{n} P(A_i)P(E|A_i) \quad \text{for } j = 1,2,3, \ldots, k$$

which is the desired result.

To illustrate how Bayes' Theorem can be used, consider the following example given by Parzen[7].

Example 7.17. Suppose, contrary to fact, there was a diagnostic test for cancer. Let A denote the event that a person tested has cancer and B denote the event that the test states that the person tested has cancer. Assume also that $P(B|A) = 0.95$ and $P(B'|A') = 0.95$. Find the probability that a person who according to the test has cancer actually has it, that is, compute $P(A|B)$. Assume that the probability that a person that has taken the test actually has cancer is given by $P(B) = .005$. Since $A \cup A' = S$ and $A \cap A' = \phi$, Bayes' Theorem implies

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A')P(A')}$$

$$= \frac{(0.95)(0.005)}{(0.95)(0.005) + (0.05)(0.995)} = \frac{0.00475}{0.00475 + 0.04975} = 0.087.$$

One should carefully consider the meanings of this result in terms of the original problem. The cancer diagnostic test was assumed to be highly reliable, since it could detect cancer in 95 per cent of the cases in which cancer was present. However, in only 8.7 per cent of the cases in which the test indicates that the person has cancer is it actually true that cancer is present.

The following example is a problem posed by Larson[8].

Example 7.19. Suppose that you are being held a political prisoner in Russia and will be exiled to either Siberia or Mongolia with probabilities .7 and .3 respectively. Suppose also that it is known that the probability of a Siberian resident wearing a seal-skin coat is .8, whereas this same event has probability .4 in Mongolia. Late one night you are blindfolded and thrown on a truck. After approximately two weeks' travel, the truck stops and your blindfold is removed. The first person you see is not wearing a seal-skin coat. What is the probability you are in Siberia? Bayes' Theorem can be used to answer this question. Let A be the event you are sent to Siberia and A' be the event you are sent to Mongolia. Let B be the event that a randomly selected resident is wearing a seal-skin coat. From the information given in the problem, $P(A) = .7$, $P(A') = .3$, $P(B|A) = .8$, and $P(B|A') = .4$. The remaining problem is to compute $P(A|B')$. Note that $A \cup A' = S$ and $A \cap A' = \phi$ so that Bayes' Theorem implies that

$$P(A|B) = \frac{P(A)P(B'|A)}{P(A)P(B'|A) + P(A')P(B'|A')} = \frac{(.7)(.2)}{(.7)(.2) + (.3)(.6)} = 7/16.$$

There has been a certain amount of confusion surrounding Bayes' Theorem. Difference of opinion exist even among experts. However, Bayes' Theorem remains a very powerful tool in many applied problems. An interesting use of Bayes' Theorem to evaluate probabilities during the course of a bridge game is given by Waugh and Waugh[8].

If A and B are two possible events in the same sample space, then the likelihood that A occurs may or may not be effected by whether or not B occurs.

Definition 7.12. Two events, A and B in the same sample space, are said to be independent iff $P(A \cap B) = P(A)P(B)$. They are called dependent events if $P(A \cap B) \neq P(A)P(B)$.

Before some concrete examples are considered, it is possible to explore the intuitive notion of independence to deduce some rather obvious results.

Theorem 7.10. If S is a sample space and $A \subset S$, then S and A are independent.

Proof: Since $A \cap S = A$, $P(S \cap A) = P(A) = P(A)P(S)$ because $P(S) = 1$. Thus, A and S are independent events.

Theorem 7.11. If A and B are disjoint events in the same sample space with $P(A) \neq 0$ and $P(B) \neq 0$, then A and B are dependent events.

Proof: If $A \cap B = \phi$, then $P(A \cap B) = P(\phi) = 0$. But, if $P(A) \neq 0$ and $P(B) \neq 0$, then $P(A \cap B) \neq P(A)P(B)$. Thus, A and B are dependent events.

Theorem 7.12. If A and B are independent events in the same sample space, then $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

Proof: If A and B are independent, then $P(A|B) = P(A \cap B)/P(B) = P(A)P(B)/P(B) = P(A)$ and $P(B|A) = P(B \cap A)/P(A) = P(B)P(A)/P(A) = P(B)$.

Example 7.20. Suppose a 13-card hand is randomly selected from a deck of 52 cards. Let A be the event that a hand containing an ace of spades is drawn. Let B be the event that a hand containing a three of clubs is drawn. Are these two events independent? If A and B are independent, then $P(A \cap B) = P(A)P(B)$. First, note that $A \cap B$ is the event that a hand contains an ace of spades and a three of clubs. So $P(A \cap B) = {}_{50}C_{11}/{}_{52}C_{13} = 1/17$. But $P(A) = {}_{51}C_{12}/{}_{52}C_{13}$ and $P(B) = {}_{51}C_{12}/{}_{52}C_{13}$ which implies that $P(A)P(B) = 1/16$. Therefore, $P(A \cap B) = 1/17 \neq 1/16 = P(A)P(B)$ which implies that A and B are dependent.

Example 7.21. Suppose that based on previous medical experiments the following probabilities have been established for a person selected at random. Let A be the event that a person smokes and B be the event that he gets cancer. Then assume $P(A \cap B) = .50$, $P(A \cap B') = .2$, and $P(A' \cap B') = .2$. Does it seem reasonable that A and B are independent? As in the last example, one must find $P(A)$, $P(B)$, and $P(A \cap B)$. Note that A can be written as $A = A \cap S = A \cap (B \cup B')$ and since $\cap$ distributes over $\cup$, $A = (A \cap B) \cup (A \cap B')$. Also, $(A \cap B) \cap (A \cap B') = \phi$, so that, $P(A) = P((A \cap B) \cup (A \cap B')) = P(A \cap B) + P(A \cap B') = .50 + .20 = .70$. Similarly, $P(B) = P(A \cap B) + P(A' \cap B) = .50 + .10 = .60$. But, $P(A \cap B) = .50$ and $P(A)P(B) = (.70)(.60)$. Therefore, $P(A \cap B) \neq P(A)P(B)$ which implies that A and B are not independent.

Much of the theory developed in this chapter can be found presented in a more advanced level in Feller[10], Parzen[11], and Larson[12]. For the reader who is interested in intriguing problems in probability, Fifty Challenging Problems in Probability by F. Mosteller[13] is an excellent reference. See the Appendix for other references.

The presentation given in this chapter is a set theoretic approach to probability in finite sample spaces. Many of the fundamental concepts involved in a study of discrete probability were considered in a somewhat simplified approach along with various applications of probability theory.

FOOTNOTES

[1] J. B. Fraleigh, Mainstreams of Mathematics (Reading, Massachusetts; 1969), p. 417.

[2] E. Parzen, Modern Probability Theory and Its Applications (New York, 1960), p. 18.

[3] Ibid., pp. 18-31.

[4] I. Niven, Mathematics of Choice: How To Count Without Counting (New York, 1965), pp. 1-160.

[5] H. F. Fehr, L. N. Bunt, and G. Grossman, An Introduction to Sets, Probability, and Hypothesis Testing (Boston, 1964), p. 214.

[6] H. J. Larson, Introduction to Probability and Statistical Inference (New York, 1969), p. 47.

[7] W. Feller, An Introduction to Probability Theory and Its Applications, Vol. I (New York, 1968), p. 36.

[8] Larson, pp. 47-48.

[9] D. F. Waugh and F. V. Waugh, "On Probabilities in Bridge," Journal of American Statistical Association, XLVIII (October, 1953), pp. 79-87.

[10] Feller, pp. 10-121.

[11] Parzen, pp. 8-91.

[12] Larson, pp. 15-61.

[13] F. Mosteller, Fifty Challenging Problems in Probability with Solutions (Reading, Massachusetts; 1965), pp. 1-88.

CHAPTER VIII

SUMMARY AND RECOMMENDATIONS

Summary

The purpose of this study was to develop enrichment topics for twelfth-grade mathematics students. The materials developed were designed for senior mathematics students who have completed a minimum of basic algebra, geometry, and advanced algebra.

The topics developed in this study were carefully selected from the topics suggested in the literature. Topics were selected from the fields of number theory, abstract algebra, topology, geometry, and probability theory to give the student a broader perspective of the domain of mathematics. The topics were also selected to emphasize many of the fundamental ideas of mathematics such as sets, relations, functions, isomorphism, and so on. The importance of the axiomatic method was stressed in the development of algebraic systems and geometric systems.

The approach used for each topic varied somewhat with the sophistication of the concepts involved. The approach to groups and graph theory was rather intuitive, while the approach to Farey fractions, fields, finite geometries, and probability was more rigorous.

In Chapter I the writer developed the background for the problem, stated the problem, explained the scope of the study, and indicated the significance of the study. Chapter II included a basic discussion of

Farey fractions and Farey sequences. The theory developed in relation to Farey fractions was used to give a rational approximation to an irrational number.

Chapter III presented an intuitive introduction to finite groups. Other related topics such as loops and braids were also discussed. Several games such as the network game and tangloids were illustrated as amusing applications to group theory. In Chapter IV an algebraic system developed as ordered triples of integers was shown to be an Archemedian ordered field isomorphic to the rational numbers. The various properties of ordered fields were investigated through the study of this one algebraic system.

Chapter V contained a discussion of various Euclidean and non-Euclidean finite geometries, while Chapter VI included a consideration of applications to graph theory. The Königsberg Bridge Problem was considered as motivation for the study of graphs. Gradually, the intuitive notion of a graph was defined more abstractly and some of the fundamental theorems of graph theory were proven. Solutions to such historically famous problems as Hamilton's Travelers Dodecahedron problem were also given. Chapter VII presented the development of a set theoretic approach to finite probability. The basic notions of probability were developed from three basic axioms and various examples were given to illustrate the theory that was developed.

Recommendations

It is recommended that the materials developed in this study be used as enrichment topics for twelfth-grade mathematics students. It is recommended that a study be conducted to determine the effectiveness of enrichment in the twelfth-grade as compared to standard acceleration with no enrichment. The study should involve a comparison of college performance, attitudes, and conception of mathematics as a science.

It is further recommended that the importance of enrichment be given strong consideration as a means for challenging the mathematically talented. It is also recommended that enrichment be given consideration in developing the twelfth-grade mathematics curriculum. Enrichment could be provided in mathematics laboratories, mathematics clubs, seminars, as well as a supplement to standard courses.

It is recommended that the relationship between constructing models for finite geometries and graph theory be investigated. That is, one may be able to characterize the model for a finite geometry from the postulate set using graph theory.

It is recommended that other enrichment topics be developed particularly from the newer areas of mathematics. For example, computer logic and programming offer excellent possibilities for enrichment topics. Other topics that have received limited attention include linear programming, convex sets, calculus of finite differences, and lattice theory.

The late G. H. Hardy once observed that there are few more popular subjects than mathematics. His contention is amply borne out by the universal interest manifested in mathematical recreations for over 2000 years.[1] As mathematical knowledge grows, the opportunities for new topics for enrichment increase. Historically, the interest in an intriguing problem in a given area of mathematics has precipitated a keen interest in the study of mathematics. For example, Euler's interest in the Königsberg Bridge Problem led to the study of graphs and many writers feel that this was the beginning of combinatorial topology.

Enrichment materials are designed to encourage and nourish the interest of young people in mathematics. Enrichment has usually been achieved by guiding students to deeper consideration of standard topics in a course of study, encouraging individual research, and organizing extra-curricular activities in the form of mathematics clubs.[2]

The materials developed in this study could be used as enrichment materials to supplement standard courses. The materials could also be used for independent study projects for particular students or groups of students in seminars as the time and interest of the students and of the teacher may make feasible. It should be noted that no teacher of mathematics, at any level, can be expected to be familiar with all areas of mathematics. Some of the topics developed in this paper may not be familiar to many high school mathematics teachers. However, these teachers should not hesitate to make a topic a joint study project. This will force a certain amount of independence upon the student since he will not be able to ask the teacher each little detail. Thus, the student must reason through the material himself with the help of additional references and limited help from the teacher.

Enrichment topics offer an excellent opportunity for individualization of instruction and for developing independent study techniques. In addition enrichment topics offer a means for introducing and reinforcing many of the basic concepts of mathematics in a different and challenging manner.

Enrichment Mathematics for High School[3], Mathematics for the Academically Talented Student in the Secondary School[4], and

Recreational Mathematics[5] contain excellent bibliographies of enrichment for high school mathematics students.

The academically talented student in mathematics will continue to be a point of concern for high school teachers and administrators. Hopefully, mathematics teachers and school administrators are cognizant of the need for more mathematically trained students. However, the exponential growth of mathematics, both theoretical and applied, does not dictate that acceleration is the only concern. Enrichment should play an important role in the mathematics curriculum of the future.

FOOTNOTES

[1] W. L. Schaaf, Recreational Mathematics (Washington, D, C.; 1963), p. 1.

[2] National Council of Teachers of Mathematics, Enrichment Mathematics for High School (Washington, D. C.; 1963), p. 2.

[3] Ibid., p. 3.

[4] J. H. Hlavaty, ed., Mathematics for the Academically Talented Student in the Secondary School (Washington, D. C.; 1959), pp. 6-16 and 379-388.

[5] Schaaf, pp. 44-48.

A SELECTED BIBLIOGRAPHY

Adler, Irving. *Groups in the New Mathematics*. New York: The John Day Company, 1967.

Allendoerfer, C. B. "The Case Against Calculus." *The Mathematics Teacher*, LII (October, 1960), pp. 451-453.

Artin, Emil. "Braids and Permutations." *Annals of Mathematics*, Second Series, XLVIII (July, 1947), pp. 643-649.

__________. "The Theory of Braids." *The Mathematics Teacher*, LII (May, 1959), pp. 328-333.

Banard, D. S. *Adventures in Mathematics*. New York: Hawthorn Books, Inc., 1967.

Blank, A. A. "Remarks on the Teaching of Calculus in the Secondary School." *The Mathematics Teacher*, LII (November, 1960), pp. 537-539.

Blumenthal, L. M. *A Modern View of Geometry*. San Francisco: W. H. Freeman and Company, 1961.

Buchanan, O. L. "Opinions of College Teachers of Mathematics Regarding Content of the Twelfth-Year Courses in Mathematics." *The Mathematics*, LVIII (March, 1965), pp. 223-225.

Busacker, R. G. and T. L. Saaty. *Finite Graphs and Networks: An Introduction with Applications*. New York: McGraw-Hill, 1965.

Commission on Mathematics of the College Entrance Examination Board. *Report of the Commission on Mathematics: Program for College Preparatory*. New York: College Entrance Examination Board, 1959.

Committee on the Undergraduate Program. *Elementary Mathematics of Sets with Applications*. Berkeley: Mathematical Association of America, 1958.

Coxford, A. F. "Geometric Diversions: A 25-Point Geometry." *The Mathematics Teacher*, LVIII (December, 1964), pp. 563-564.

Crouch, Ralph and David Beckman. *Algebraic Systems*. Glennview, Illinois: Scott Foresman, 1966.

Cundy, H. M. "25-Point Geometry." *Mathematical Gazette*, XXXVI (September, 1952), pp. 159-165.

Eves, Howard and C. V. Newsom. *An Introduction to the Foundations and Fundamental Concepts of Mathematics*. New York: Holt, Rinehart and Winston, 1965.

Fehr, H. F., L. N. Bunt, and G. Grossman. *An Introduction to Sets, Probability, and Hypothesis Testing*. Boston: D. C. Heath and Company, 1964.

Feller, William. *An Introduction to Probability Theory and Its Applications*, 2nd ed., Vol. 1. New York: John Wiley and Sons, Inc., 1957.

Ferguson, W. E. "Calculus in the High School." *The Mathematics Teacher*, LIII (October, 1960), pp. 451-453.

Filippone, S. R. "A Course of Basic Mathematical Concepts for Advanced High School Students." *The Mathematics Teacher*, LIII (April, 1960), pp. 256-259.

Fraleigh, J. B. *Mainstreams of Mathematics*. Reading, Massachusetts: Addison-Wesley, 1969.

Golos, E. B. *Foundations of Euclidean and Non-Euclidean Geometry*. New York: Holt, Rinehart and Winston, 1968.

Grossman, George. "Advanced Placement Mathematics for Whom." *The Mathematics Teacher*, LV (November, 1962), pp. 560-566.

Grossman, Israel and Wilhelm Magnus. *Groups and Their Graphs*. New York: Random House, Inc., 1964.

Hardy, G. H. "A Mathematician's Apology." *The World of Mathematics*. Ed. J. R. Newman. New York: Simon and Schuster, 1956, pp. 2027-2038.

Heidlage, Martha. "A Study of Finite Geometry." *The Pentagon*, XXII (Fall, 1963), pp. 18-27.

Hlavaty, J. E., ed. *Mathematics for the Academically Talented Student in the Secondary School*. Washington, D. C.: National Education Association, 1959.

Hollingstead, Irving. "Number Theory--A Short Course for High School Seniors." *The Mathematics Teacher*, LX (March, 1967), pp. 222-227.

Laatsch, Richard. *Basic Algebraic Systems: An Introduction to Abstract Algebra*. New York: McGraw-Hill, 1968.

Larson, H. J. *Introduction to Probability Theory and Statistical Inference*. New York: John Wiley and Sons, Inc., 1969.

MacNeish, H. F. "Four Finite Geometries." *The American Mathematical Monthly*, XLIX (January, 1942), pp. 15-21.

McKillip, W. D. "The Effects of High School Calculus on Students' First Semester Calculus Grade at the University of Virginia." *The Mathematics Teacher*, LIX (May, 1966), pp. 470-472.

Meserve, B. E. *Fundamental Concepts of Geometry*. Cambridge, Massachusetts: Addison-Wesley Publishing Company, Inc., 1955.

Mosteller, Frederick. *Fifty Challenging Problems in Probability with Solutions*. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 1965.

National Council of Teachers of Mathematics. *Enrichment Mathematics for High School*, Twenty-Eighth Yearbook. Washington, D. C.: The Council, 1963.

Niven, Ivan. *Mathematics of Choice*. New York: Random House, Inc., 1965.

Ore, Oystein. *Graphs and Their Uses*. New York: Random House, Inc., 1963.

Parzen, Emanuel. *Modern Probability Theory and Its Applications*. New York: John Wiley and Sons, Inc., 1960.

Richardson, Moses. *Fundamentals of Mathematics*. New York: The MacMillan Company, 1941.

Schaaf, W. L. *Recreational Mathematics*. Washington, D. C.: The National Council of Teachers of Mathematics, 1963.

School Mathematics Study Group. *Mathematics for High School*. New Haven: Yale University Press, 1962.

Stein, S. K. *Mathematics: The Man-made Universe*. San Francisco: W. H. Freeman and Company, 1963.

Watson, Donald. "Condition for a Loop to be a Group." *The American Mathematical Monthly*, LXXIV (September, 1967), pp. 843-844.

Woodby, L. G. *Emerging Twelfth-Grade Mathematics Programs*. Washington, D. C.: U. S. Government Printing Office, 1965.

Wylie, C. R. *Foundations of Geometry*. New York: McGraw-Hill, 1964.

Zant, J. H., ed. *Improvement of Mathematics Instruction in Oklahoma Grades K-12*. Oklahoma City: Oklahoma State Department of Education, 1967.

Zassenhaus, Hans. *The Theory of Groups*. New York: Chelsea, 1949.

APPENDIX

COLLATERAL REFERENCES

COLLATERAL REFERENCES

Farey Fractions

Bester, A. H. Recreation in the Theory of Numbers. New York: Dover Publications, Inc., 1964.

Hardy, G. H. and E. M. Wright. An Introduction to the Theory of Numbers. Oxford: Clarendon Press, 1936. (pages 23-30)

Neville, E. H. "The Structure of Farey Series." Proceedings London Mathematical Society, LI (November, 1946), pp. 132-144.

Olds, C. D. Continued Fractions. New York: Random House, Inc., 1963. (pages 123-127)

Lucas and Fibonacci Numbers

Alfred, U. "On Square Lucas Numbers." The Fibonacci Quarterly, II (February, 1964), pp. 11-12.

Basin, S. L. "A Primer on the Fibonacci Sequence." The Fibonacci Quarterly, I (April, 1963), pp. 65-67.

Brooke, M. "Fibonacci Numbers: Their History Through 1900." The Fibonacci Quarterly, II (April, 1964), pp. 149-153.

Hoggote, V. E. Fibonacci and Lucas Numbers. Boston: Houghton Mifflin Company, 1969.

Schaaf, W. L. Recreation Mathematics. Washington, D. C.; National Council of Teachers of Mathematics, 1963. (pages 48-50 contains 39 references to Fibonacci numbers)

Vorobiv, N. N. Fibonacci Numbers. New York: Blaisdell Publishing Company, 1962.

Groups

Burnside, W. Theory of Groups of Finite Order. New York: Dover Publications, Inc., 1911 (advanced approach).

Carmidail, R. D. *Introduction to the Theory of Groups of Finite Order*. Boston: Ginn and Company, 1937. New York: Dover Publications, 1956. (Paperback)

Coteter, H. S. M. and W. O. J. Moser. *Generators and Relations for Discrete Groups*. New York: Springer Verlog, 1957. (Chapter 3 includes graphs, maps, and Caley diagrams)

Fraleigh, J. B. *Mainstreams of Mathematics*. Reading, Massachusetts: Addison Wesley Publication Company, 1969. (pp. 129-175)

Gardner, K. L. *Discover Modern Algebra*. Oxford: Oxford University Press, 1966. (A good reference--written on a rather elementary level)

Ingraham, M. L. "A Permutation Group and Its Isomorphs." *Enrichment Mathematics for High School*. Washington, D. C.: National Council of Teachers of Mathematics, 1963. (pages 150-161)

Lederman, W. *Introduction to the Theory of Finite Groups*. New York: Oliver and Boyd, 1949.

Miller, G. A., H. F. Blichfeldt, and L. E. Dickson. *Theory and Application of Finite Groups*. New York: Dover Publications, Inc., 1961.

Fields

Crouch, R. and D. Beckman. *Algebraic Systems*. Glennview, Illinois: Scott, Foresman and Company, 1966. (pages 227-289--has many examples and problems related to fields)

Earl, B., J. W. Moore, and W. I. Smith. *Groups and Fields*. New York: McGraw Hill Book Company, Inc., 1963.

Perfect, H. *Topics in Algebra: A Selection for Sixth Forms*. Oxford: Pergmon Press, 1966.

Lawvere, F. W. *The Language of Algebra: Fields and Ordered Fields*. Chicago: Encyclopedia Britannica Press, 1960. (A TEMAC-Programmed Learning publication--gives a rather complete treatment of fields, Chapters XII and XV--Models of fields and ordered fields--are of particular interest)

Sawyer, W. W. *A Concrete Approach to Abstract Algebra*. San Francisco: W. H. Freeman and Company, 1959. (pages 26-31 and 71-77)

Finite Geometry

Banks, J. H. *Elements of Mathematics*. Boston: Allyn and Bacon, Inc., 1969.

Blumenthal, L. M. *A Modern View of Geometry*. San Francisco: W. H. Freeman and Company, 1961.

Coxeter, H. S. M. *Introduction to Geometry*. New York: John Wiley and Sons, 1961.

Edge, W. L. "31-Point Geometry." *Mathematical Gazette*, XXXIX (May, 1955), pp. 113-121.

Eves, H. *A Survey of Geometry*. Boston: Allyn and Bacon, Inc., 1963. (pages 325-436)

Miller, W. A. "A Construction of a Physical Model for Finite Euclidean and Projective Geometries." *The Mathematics Teacher*, LXIII (April, 1970), pp. 301-306.

Mitchell, H. H. "Linear Groups and Finite Geometries." *American Mathematical Monthly*, ILVII (March, 1935), pp. 592-603.

Room, T. G. *A Background to Geometry*. Cambridge: Cambridge University Press, 1967. (pages 85-93, advanced discussion of when it is possible for a finite geometry to exist, i.e., for what sets of points and lines.)

Veblen, O. and J. W. Young. *Projective Geometry*. Boston: Ginn and Company, 1910.

Graphs and Related Topics

Arnold, B. H. *Intuitive Concepts in Elementary Topology*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1962. (pages 22-43)

Ball, W. R. *Mathematical Recreation and Essays*. New York: Macmillan Publishing Company, 1962.

Barr, S. *Experiments in Topology*. New York: Thomas Cornell Company, 1964.

Bodino, A. *Economic Applications of the Theory of Graphs*. New York: Gordon and Breach, 1962.

Franklin, P. *The Four Color-Problem*. New York: Script Mathematics, Yeshiva University Press, 1961.

Gardner, M. *Mathematical Puzzles and Diversions*. New York: Simmon and Schuster, 1961. (Chapter 7--Recreation Topology--network tracing and knots)

Kasner, E. and J. Newman. *Mathematics and Imagination*. New York: Simmon and Schuster, 1963. (Chapter 8--Rubber Sheet Geometry)

National Council of Teachers of Mathematics. *Enrichment Mathematics for High School*. Washington, D. C.: N. C. T. M., 1963. (Section 7--Nets; Section 25--Knots and Wheels)

Probability

Chernoff, H. and L. Moses. *Elementary Decision Theory*. New York: John Wiley and Sons, Inc., 1959.

Copeland, A. H. "Fundamental Concepts of the Theory of Probability." *American Mathematical Monthly*, ILVIII (April, 1941), pp. 522-530.

Hodges, J. L. and E. L. Lehmann. *Basic Concepts of Probability and Statistics*. San Francisco: Holden-Day, 1964.

Hogben, L. *Chance and Choice by Cardpack and Chessboard: An Introduction to Probability in Practice by Visual Aids*. New York: Chantideer Press, 1950.

National Council of Teachers of Mathematics. *Enrichment Mathematics for High School*. Washington, D. C.: N.C.T.M., 1963. (pages 329-339--The Best or the Probable Best, pages 285-301--Random Walks)

National Council of Teachers of Mathematics. *Insights Into Modern Mathematics*. Washington, D. C.: N.C.T.M., 1957, pages 336-371. (depends on knowledge of calculus)

Neyman, J. *First Course in Probability and Statistics*. New York: Holt, Rinehart and Winston, 1950.

Schaaf, W. L. *Recreational Mathematics*. Washington, D. C.: National Council of Teachers of Mathematics, 1963. (over 100 references on Probability, Gambling, and Game Strategy--pages 124-131)

VITA

2

Hiram Drexel Johnston

Candidate for the Degree of

Doctor of Education

Thesis: SUGGESTED MATHEMATICS ENRICHMENT TOPICS FOR HIGH SCHOOL SENIORS

Major Field: Secondary Education

Biographical:

Personal Data: Born in Stillwater, Oklahoma, August 12, 1941, the son of Mr. and Mrs. Drexel E. Johnston.

Education: Attended grade school and high school in Stillwater, Oklahoma; graduated from Stillwater High School in 1959; received the Bachelor of Science degree from Oklahoma State University in May, 1963; received the Specialist in Education degree from Oklahoma State University in August, 1969, with a major in Secondary Education; completed the requirements for the Doctor of Education degree at Oklahoma State University in July, 1970.

Professional Experience: Employed as mathematics teacher at C. E. Donart High School, Stillwater, Oklahoma, summer, 1963; served as an officer in the U. S. Army from September, 1963, to September, 1966; accepted a Prospective Teacher Fellowship and attended Oklahoma State University from September, 1966, to August, 1968; graduate assistant in the department of mathematics at Oklahoma State University, 1968 through 1970.