NASA/TP—2003-212088

Concepts of Mathematics for Students of Physics and Engineering: A Dictionary

Joseph C. Kolecki
Glenn Research Center, Cleveland, Ohio

August 2003

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the Lead Center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at 301–621–0134

- Telephone the NASA Access Help Desk at 301–621–0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076

NASA/TP—2003-212088

Concepts of Mathematics for Students of Physics and Engineering: A Dictionary

Joseph C. Kolecki
Glenn Research Center, Cleveland, Ohio

National Aeronautics and
Space Administration

Glenn Research Center

August 2003

Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22100

Available electronically at http://gltrs.grc.nasa.gov

Table of Contents

Concepts of Mathematics for Students of Physics and Engineering: A Dictionary

Joseph C. Kolecki
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Summary

A physicist with an engineering background, the author presents a mathematical dictionary containing material encountered over many years of study and professional work at NASA. This work is a compilation of the author's experience and progress in the field of study represented and consists of personal notes and observations that can be used by students in physics and engineering.

Introduction

Mathematics is an endless field of study, and no one publication can encompass it or even begin to. Although the present book makes no such claims, the reader may ask, Why write such a mathematics dictionary at all when there are numerous ones on the market? The answer is that dictionaries differ: formal dictionaries function as research tools and reflect differences in approach depending upon the authors' goals. Authors of formal dictionaries attempt to reach the widest audience. Personal dictionaries are not so constrained because they can be reorganized to reflect the authors' progress in a field of study. They are compilations of personal notes and observations that can be used to provide material for future work and publications.

I have found that a useful way to keep notes and organize my thoughts is to compile them in a personal lexicon where I write the definitions and organize the materials as I understand them, a sort of journaling. For the past 30 years in the various fields of study attempted, journaling has facilitated organization and long-term retention; I was able to recognize that I needed to fill gaps in my knowledge and understanding.

The appendixes are a compendium of additional topics, the contents of which are too large to be included as individual citations. I have compiled compendia such as these ever since high school to enable me to rationally organize material from a variety of areas and to supplement missing information in published material. For example, the material in appendix H, Definitions and Theorems From Calculus, enabled me to see the actual lay of the land without worrying about the complex supporting arguments and proofs. The beauty in mathematical theorems can be seen most clearly when they are treated in this manner.

This mathematics dictionary is one of three that I compiled over the years and is the most complete, my intentions having been to publish it for two reasons: the first is that the material contained herein represents areas of knowledge I had to assimilate and apply when called upon. As a physicist with an engineering background, my work encompassed both fields. Therefore, this information should be of some use to students in these fields. The second reason is that the organization of this dictionary reflects the working of one man's mind and therefore serves as a model for others who wish to compile their own volumes.

Logic and Reasoning

induction. A process of reasoning in which a general conclusion is drawn from a set of particular premises. The premises are often based on experience or experimental evidence; the conclusion goes beyond the information contained in the premises and does not follow necessarily from them. An inductive argument may be highly probable but may lead from true premises to false conclusions: *A large number of sightings might be used to inductively prove that all swans are white*.

deduction. A process of reasoning in which a conclusion follows necessarily from given premises so that it cannot be false when the premises are true: *All men are wise; Socrates is a man; therefore, Socrates is wise*.

argument. A process or instance of inductive or deductive reasoning that purports to show its conclusion to be true; an argument may consist of a sequence of statements, one of which is the conclusion and the rest of which are the premises.

valid argument. One in which the truth of the premises ensures the truth of the conclusion. An inference is formally valid when it is justified by the form of the premises and the conclusion alone: *Tom is a bachelor; therefore, Tom is unmarried* (valid but not formally valid)*; Today is hot and dry; therefore, today is hot* (formally valid).

conclusion. A statement that purports to follow from another statement or other statements (the premises) by means of an argument or proof.

proof. A sequence of statements, each of which is (1) either an axiom or an assumption, (2) is validly derived from those statements preceding it, or (3) is the conclusion, a statement whose truth is thereby established.

direct proof. One that proceeds linearly from the premises to the conclusion. It may argue directly from an implication $p \Rightarrow q$ or its contrapositive $\sim p \Rightarrow \sim q$. An equivalency proof $p \Leftrightarrow q$ must prove both $p \Rightarrow q$ and $q \Rightarrow p$.

indirect proof (reducio ad absurdum)**.** One that assumes the falsehood of the desired conclusion and shows the assumption to be impossible, usually by arriving at a logical contradiction.

axiom. A statement stipulated to be true for the purposes of constructing a mathematical system in which theorems may be derived by certain rules of inference.

assumption. A statement taken to be true for the purposes of a particular argument and used as a premise to infer its consequences.

premise. A statement from which a conclusion is drawn in a particular argument. It may be an axiom of the relevant theory or merely an assumption taken to be true for the purposes of discovering its consequences.

theorem. A statement that can be deduced from the axioms of a mathematical system by a recursive application of certain rules of inference.

lemma. A subsidiary result proved to simplify the proof of a required theorem.

corollary. A proposition that follows directly from the statement or the proof of another proposition. A corollary is a subsidiary theorem.

Sets

set S**.** A collection of elements (more formally, points) s (members) with some defined property or properties. Given any candidate element s^*, it may be determined from the properties of s^* and the defined property or properties required for membership in S, whether s^* is an element of S; e.g., let $S = \{(x,y)|x^2 + y^2 = 1\}$; then $s^* = (0,1)$ is a member of S but $s^* = (2,3)$ is not. A set may be represented in tabular form as $S = \{a,e,i,o,u\}$ or in set builder notation as $S = \{x|x \text{ is even}\}$, which reads "the set of all x such that x is even."

complement S^C **of a set** S**.** The set of all elements not contained in S and represented as $S^C \equiv \{x|x \notin S\}$.

universal set U**.** The union of any set S and its complement and represented as $U = S \cup S^C$ and $S^C = \mathrm{U} \backslash S$.

null set or ***empty set*** Φ**.** A set that contains no elements. The set Φ is not to be confused with the set $\{\Phi\}$ that contains one element, Φ.

equal sets. Two sets S and T that are equal if they contain the same elements. If a given element appears n times in a given set, it is counted only once as a unique element. Equal sets are represented as $S = T \Leftrightarrow (S \subset T) \wedge (T \subset S)$: the sets $\{a,a,b,b,b\}$ and $\{a,b\}$ are considered equal.

union $S \cup T$ **of two sets** S **and** T**.** The set that contains all the elements in S and all the elements in T and is represented as $S \cup T \equiv \{x|x \in S \text{ or } x \in T\}$. As a set operation, union is idempotent (i.e., $A \cup A = A$), commutative, and associative. The null set is an identity element for set union (i.e., $A \cup \Phi = A$). Set union is distributive over set intersection.

intersection $S \cap T$ **of two sets** S **and** T**.** The set that contains only those elements common to both sets. If the intersection of S and T is the null set, then S and T are called "disjoint" and are represented as $S \cap T \equiv \{x|x \in S \text{ and } x \in T\}$. As a set operation, set intersection is idempotent, commutative, and associative. The null set is a zero element for set

intersection (i.e., $A \cap \Phi = \Phi$). Set intersection is distributive over set union.

difference $S \backslash T$ of two sets S and T**.** The set which includes all members of the first set that are not members of the second set, represented as $S \backslash T \equiv \{x | x \in S \text{ and } x \notin T\}$.

symmetric difference $S \Delta T$ of two sets S and T**.** The set of all elements that belong to either but not both of the sets and represented as $S \Delta T \equiv \{x | x \in (S \cup T) \backslash (S \cap T)\}$. As a set operation, the symmetric difference is commutative and associative. The null set is a zero element for symmetric difference (i.e., $S \Delta S = \Phi$ and $S \Delta \Phi = S$). Additionally, $S \Delta S^C = U$ and $S \Delta U = S^C$. Set intersection is distributive over symmetric difference.

Cartesian product $S \times T$ of two sets S and T**.** The set of all ordered pairs (s,t), where s is an element from the first set in the product and t is an element from the second, represented as $S \times T \equiv \{\text{Ordered pairs } (s,t) | (s \in S) \text{ and } (t \in T)\}$: the real number spaces R^n are Cartesian products of R with itself n times. Thus, $R = R^1$ (the real line); $R \times R = R^2$ (the Cartesian or complex planes); $R \times R \times R = R^3$ (Euclidean or Cartesian three-space), etc. As a set operation, the Cartesian product is distributive over set union, set intersection, and set difference.

subset of a set T**.** Any set $S \subset T$ whose elements are also in S. The null set is a subset of every set, and every set is a subset of itself; i.e., for any set T, $\Phi \subset T$ and $T \subset T$.

proper subset of a set T**.** Any subset of T other than T itself: if $S \subset T$ and $S \neq T$, then S is a proper subset of T or $(S \subset T) \wedge (S \neq T) \Rightarrow S$ is a proper subset of T.

partition of a set S**.** Any collection of nonempty subsets of S such that every element of S belongs to exactly one of the subsets in the collection. Thus, S is the union of these subsets, and any two distinct subsets are disjoint.

refinement of a partition**.** Another partition constructed by further subdividing the members of the original partition.

interior of a set S**.** The largest open subset of S equal to the union of all the open subsets contained within S: if $\{S_i\}$ is the set of all open subsets of a set S, then the interior of S is the set I_s defined by $I_s = \cup_{i=1}^{n} = S_i$, where n is the number of open subsets.

superset of a set S**.** Any set that contains S as a subset.

extension of a set S**.** A superset of S in which S, along with any operations defined on S, are contained (preserved) as a subset: the extension of the real numbers is the complex numbers; the extension of the vectors is the tensors.

class C**.** A set whose elements are other sets having a specified property.

power set 2^S of a set S**.** The class of all subsets of S, including Φ and S: if S contains n-elements, then the power set of S contains 2^n-elements.

point. An element of a set (particularly in the topology of point sets).

interior point of a set S**.** Any point in an open subset of S: 0.5 is an interior point of the interval [0,1] whereas 0 is not.

boundary point of a set S**.** Any point common to both S and S^C.

exterior point of a set S**.** Any point that is neither an interior point nor a boundary point of S.

neighborhood of a point s in a set S**.** A subset of S containing s. An open neighborhood is an open set; a closed neighborhood is a closed set; a punctured neighborhood is a neighborhood (open or closed) with s deleted.

cluster point of a set S**.** A point for which any punctured open neighborhood contains other points of S. Equivalently, a cluster point of a set S is a point for which any open neighborhood has a nonempty intersection with S. A closed set contains all its cluster points.

isolated point of a set S**.** Any point that is not a cluster point in S. An isolated point has at least one punctured neighborhood that does not intersect S.

discrete set S**.** A set with no cluster points: every point is isolated; the integers are discrete, but the rationals are not since they are dense in the reals.

closed set. A set consisting of interior points and boundary points. A set in a topology is closed if it contains all its limit points. The *intersection* of any number of closed sets is a closed set. The *union* of two (or a finite number of) closed sets is a closed set.

closure of a set S**.** The smallest closed set containing S (equal to the intersection of all the closed sets containing S). The closure of the positive integers under subtraction is the set of all integers.

exterior of a set**.** The complement of its closure or the interior of the complement of the set.

boundary or ***frontier*** of a set**.** The set of points that are members of the closure of the given set and the

closure of its complement. Equivalently, the boundary of a set is the set of points in the closure but not in the interior of the set. The frontier of the half-open interval (0,1] is the set {0,1}; the frontier of the rationals is the set of all real numbers.

open set. A set consisting solely of interior points. The *intersection* of two (or a finite number of) open sets is an open set. The *union* of any number of open sets is an open union. The *complement* of a closed set is an open set. The *complement* of an open set is a closed set.

connected set. A set that cannot be partitioned into two nonempty open subsets, each of which has no points in common with the closure of the other. The rationals are not connected, but the reals are.

connected set S of real numbers. A set that has any two elements a and b with the element c (also $\in S$) lying between them.

disconnected sets. Two sets that are not connected. Any punctured neighborhood of the reals is disconnected as is the cut interval $(-1,1)/\{0\}$.

separable set. A set that contains a countable, dense subset. Any Euclidean n-space is separable because it contains rational n-tuples that are countable and dense.

separated sets. Two sets whose closures have a null intersection.

dense-in-itself set. A set for which every point is a cluster point.

dense set S. A set whose closure contains S. Given: two sets, S and T; S is dense in T if T is contained in the closure of S. Let S = {rationals} and T = {reals}; then S is dense in T since the reals are contained in the closure of the rationals.

bounded set. A set with an upper and lower bound. An upper bound is a point (number) greater than all other points in the set. A lower bound is a point (number) less than all the other points in the set.

compact set. A set that is closed and bounded. The interval [0,1] is compact; the interval (0,1) is not.

one-to-one correspondence between two sets**.** A relation in which each element of the first set corresponds to one and only one element of the second, and each element of the second corresponds to one and only one element of the first.

countable set. A set whose elements may be put into one-to-one correspondence with a subset of the natural numbers.

finite set. A set whose elements can be put into a one-to-one correspondence with a bounded initial segment of the natural numbers; i.e., a set whose elements can be counted using a terminating sequence of natural numbers.

infinite set. A set that can be put into one-to-one correspondence with a proper subset of itself.

denumerable or ***countable but infinite set.*** An infinite set that can be put into one-to-one correspondence with the natural numbers. The rationals are denumerable.

nondenumerable set. An infinite set that cannot be put into a one-to-one correspondence with the natural numbers. The reals are nondenumerable as is the closed interval [0,1].

ideal I. A nonempty family of subsets of U in which $(S \in I) \wedge (T \subset S) \Rightarrow T \in I$ and $(S \in I) \wedge (T \in I) \Rightarrow (S \cup T) \in I$. The power set of any given set is an ideal.

filter F. A nonempty family of subsets of U in which $(S \in F) \wedge (S \subset T) \Rightarrow T \in F$ and $(S \in F) \wedge (T \in F) \Rightarrow (S \cap T) \in F$. The family of all sets such that $S \subset T \subset U$ is a filter.

cover of a given set S**.** A collection of sets whose union completely contains S. An open (closed) cover is a cover that uses open (closed) covering sets.

Logical Sentences and Truth Sets

sentence. A logical statement in words or symbols.

formula. A sequence of symbols involving at least one variable x, such as $p(x)$ or $q(x)$.

variable. An expression with unspecified meaning: x = *It is…* or x = *some number.*

value. An expression with specified meaning: x_0 = *It is raining* or $x_0 = 2$.

statement. Any sentence in which the variable takes on a specific value, such as $p(x_0)$ or $q(x_0)$, and has a truth value, true or false.

negation. A statement $\sim p(x_0)$ that denies the truth of $p(x_0)$ and is of the form not $p(x_0)$.

truth set or ***solution set*** for a formula $p(x)$**.** The set $P = \{x|p(x) \text{ is true}\}$.

conjunction $p \wedge q$. Any statement of the form "$p(x_0)$ and $q(x_0)$." The conjunction $p \wedge q$ is true if $p(x_0)$ and $q(x_0)$ are both true; it is otherwise false. The truth set of $p \wedge q$ is the set $P \cap Q$ (where Q is the truth set of $q(x)$).

disjunction $p \vee q$**.** Any statement of the form "Either $p(x_0)$ or $q(x_0)$ or $p(x_0)$ and $q(x_0)$." The disjunction $p \vee q$ is false if $p(x_0)$ and $q(x_0)$ are false; it is otherwise true. The truth set of $p \vee q$ is the set $P \cup Q$.

implication $p \Rightarrow q$**.** Any statement of the form "$p(x_0)$ implies $q(x_0)$." The implication $p \Rightarrow q$ is false (or $\sim(p \Rightarrow q)$ is true) if $p(x_0)$ is true but $q(x_0)$ is false; it is otherwise true. The truth set of an implication is $P \subset Q$.

equivalence $p \Leftrightarrow q$ or p if and only if q (p iff q)**.** Any statement of the form "$p(x_0)$ implies $q(x_0)$ and $q(x_0)$ implies $p(x_0)$." The equivalence $p \Leftrightarrow q$ is true if either $p(x_0)$ and $q(x_0)$ are true or $p(x_0)$ and $q(x_0)$ are false; it is otherwise false. The truth set of an equivalence is $P = Q$.

universal quantifier $\forall$**.** A statement that reads "For all…" In any statement of the form "$\forall x$, $p(x)$" is a statement with a bound variable x, not a formula.

existential quantifier $\exists \ldots \ni \ldots$**.** A statement that reads "There exists…such that…" Any statement of the form "$\exists x \ni p(x)$" is a statement with a bound variable x, not a formula.

bound variable. Any variable specified by a quantifier: *In* $\forall x$, $p(x,y)$, *x is bound*, *y is unbound*.

universal and ***existential statements.*** Statements involving the universal and/or existential quantifiers and bound variables, such as $\forall x$, $p(x)$, or $\exists x \ni p(x)$.

negation of a ***universal statement.*** An existential statement: $\sim[\forall x, p(x)] \Leftrightarrow [\exists x \ni \sim p(x)]$.

negation of an ***existential statement.*** A universal statement: $\sim[\exists x \ni p(x)] \Leftrightarrow [\forall x, \sim p(x)]$.

contrary of a ***universal statement.*** Another universal statement: $\forall x$, $p(x) \Rightarrow q(x)$ and $\forall x$, $p(x) \Rightarrow \sim q(x)$ are contrary statements.

contrary of an ***existential statement.*** Another existential statement: $\exists x \ni p(\mathrm{x}) \wedge q(x)$ and $\exists x \ni p(x) \wedge \sim q(x)$ are contrary statements (or in some usages, subcontrary statements).

contradiction of a ***universal statement.*** An existential statement: $\forall x$, $p(x) \Rightarrow q(x)$ and $\exists x \ni p(x) \wedge \sim q(x)$ are contradictory statements (also, $\forall x$, $p(x) \Rightarrow \sim q(x)$ and $\exists x \ni p(x) \wedge q(x)$).

Numbers

natural number. One of a unique sequence of elements used for counting a collection of individuals: 1, 2, 3,… A natural number is defined as a cardinal number. Natural numbers are closed under addition and multiplication; they include an identity element for multiplication (i.e., 1, since $1 \times n = n$ for any natural number n) but none for addition. Natural numbers also include the prime numbers, perfect numbers, amicable numbers, and other types. The set of natural numbers is denoted N.

cardinal number. A measure of the size of a set that does not take into account the order of its members. The cardinal number of a set is the largest member of the sequence of natural numbers 1, 2, 3, … that corresponds member for member to the elements of the set. Two sets are equivalent if they have the same cardinal number. For example, the members of set $\{a,b,c\}$ may be put into one-to-one correspondence with the members of set $\{1,2,3\}$. The two sets are therefore equivalent; the cardinal number of each is 3. Arithmetic may be defined in terms of cardinal numbers.

ordinal number. A measure of a set that takes into account the order as well as the number of its members. The set $\{a_1,a_2,a_3\}$ is ordinally similar to the set $\{1,2,3\}$.

Other number systems are derived by extension from the natural numbers:

whole number. One that includes a natural number and the element zero: 0,1,2,3,… A whole number is closed under addition and multiplication; it includes an identity element for addition (i.e., 0, since $0 + n = n$ for any whole number n). The set of whole numbers is denoted W.

integer. A number that includes the positive whole numbers and the negative whole numbers: –3, –2, –1, 0, 1, 2, 3,… An integer is closed under addition, multiplication, and subtraction but not division since $2 \div 3$ is not an integer. The set of integers is denoted Z.

rational number. One that includes the integers and integer ratios such as 1/2, 2/5,… A rational number is closed under addition, multiplication, subtraction, and division. All rational numbers are algebraic numbers in that they are all solutions to finite algebraic equations of the form $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0$ where the a_i are rational coefficients and n is an integer. A rational number, however, is not algebraically

closed since the algebraic equation $x^2 - 2 = 0$ has no rational solution. The set of rational numbers is denoted Q.

irrational number. One that includes all numbers which are not rational numbers, such as $\sqrt{2}$. The equation $x^2 - 2 = 0$ has an irrational solution. Irrational numbers, therefore, include algebraic numbers but also include transcendental numbers. Transcendental numbers are numbers such as π and e (base of the Naperian logarithms) that are solutions to no finite algebraic equations of the form $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0$ with rational coefficients. Transcendental numbers are solutions of transcendental equations such as $\sin(x) = 0$ where $x = n\pi$ with n an integer, or $\ln(x) = 1$ where $x = e$. But the algebraic representations of $\sin(x)$ and $\ln(x)$ are infinite series of the form $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$ with all a_i rational. The set of irrational numbers is denoted Q'.

Dedekind cut. A partition of a sequence into two disjoint subsequences, all the members of one being less than those of the other. The Dedekind cut may be used to define the irrational numbers in terms of rational-number-sequence pairs. For example, $\sqrt{2}$ is defined as the pair

$$\left[\left\{x \middle| x^2 > 2\right\}, \left\{x \middle| x^2 < 2\right\}\right] \qquad (1)$$

real number. One that includes rational numbers and irrational numbers. A real number is not algebraically closed since the algebraic equation $x^2 + 2 = 0$ has no real solution. A real number is represented as a point on the real line, number line, or continuum. The set of real numbers itself is also called the continuum. The set of real numbers is denoted R.

complex number. One that includes the real numbers and all numbers which have $\sqrt{(-1)}$ as a factor. A complex number is usually represented as $z = x + jy$ with $j = \sqrt{(-1)}$. The term x is called the real part of z, $Re(z)$; the term y is called the imaginary part of z, $Im(z)$. The complex number z may also be represented as $z = \rho e^{j\theta}$ where $\rho = (x^2 + y^2)^{1/2}$ and $\theta = \arctan(y/x)$ are polar coordinates and $e^{j\theta} = \cos(\theta) + j\sin(\theta)$. The term ρ is called the modulus of z; the term θ is called the amplitude of z. A complex number is algebraically closed and is represented as a point on a Cartesian plane called an Argand diagram or Gaussian plane in which $z = (x,y)$ with $x = Re(z)$ and $y = Im(z)$. If polar coordinates are used, then $z = (\rho,\theta)$. The set of complex numbers is denoted C.

transfinite number. A cardinal or ordinal number used in the comparison of infinite sets. The smallest transfinite cardinal is $\aleph_0$ and the smallest transfinite ordinal is ω. A set has cardinality $\aleph_0$ when its elements can be put into one-to-one correspondence with the set of natural numbers. A set with cardinality $\aleph_0$ is a denumerable set. The sets of positive integers, of rationals, and of reals are each denumerable, but the set of reals (the continuum) is not. The continuum hypothesis states that the continuum has the smallest nondenumerable cardinality. This hypothesis is undecidable because both it and its negation are consistent with the standard axioms of set theory. The generalized continuum hypothesis states that for any infinite cardinal, the next greater cardinal is that of its power set.

Primes and Factors

composite number. One that may be uniquely written as a product of prime numbers: $15 = 3 \times 5$ and $144 = 32 \times 42$.

zero. A number that may not be a factor of any number other than itself since $0 \times s = 0$ for all s. Also, zero is not a unique factor since $0 = 0^2 = 0^3 = \ldots = 0^n$ for all n; 1 is a factor of all natural numbers but is also not a unique factor since $1 = 1^2 = 1^3 = \ldots = 1^n$ for all n.

Euclid's argument for the number of primes. Let $p_1 \ldots p_n$ represent the first n prime numbers. Now, form the number

$$p_1 \times p_2 \ldots \times p_n + 1 \qquad (2)$$

None of the $p_1 \ldots p_n$ can be factors of $p_1 \times p_2 \times \ldots p_n + 1$ since, upon division, they will all leave a remainder of one. Therefore, there must be either a prime factor of $p_1 \times p_2 \times \ldots \times p_n + 1$ which is $> p_n$ or the number $p_1 \times p_2 \times \ldots \times p_n + 1$ must itself be prime. In either case, whatever value of n is chosen, a prime

number larger than p_n must exist. The number of primes is therefore infinite.

Mersenne prime. Any prime number of the form $2^n - 1$ where n is an integer. Define a number $M_n = 2^n - 1$. It may be shown that if n is composite, then M_n is composite; however, if M_n is prime, then n is prime (N.B., this argument uses the theorem of the contrapositive). Thus, n = prime is a necessary condition for M_n = prime.

If n is composite (i.e., $n = ab$), then $2^a - 1$ and $2^b - 1$ are factors of M_n. One may show that $2^a - 1$ is a factor of M_n by constructing a trial case and then generalizing. Begin by choosing $b = 3$. Then $n = 3a$ and

$$\frac{2^{3a}-1}{2^a-1} = 2^{2a} + 2^a + 1 \qquad (3)$$

The division is exact. This trial (and others like it) suggests the general solution:

$$\frac{2^{ab}-1}{2^a-1} = 2^{(b-1)a} + 2^{(b-2)a} + \ldots + 2^{2a} + 2^a + 1 \qquad (4)$$

which is also exact. A similar argument may be made for division by $2^b - 1$.

perfect number. One whose divisors (including 1) add to give twice the number: 28 is a perfect number because its divisors 1, 2, 4, 7, 14, and 28 add to give

$$1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \times 28 \qquad (5)$$

Any number of the form $2^c(2^{c+1} - 1)$ is a perfect number if $2^{c+1} - 1$ is a Mersenne prime.

Fermat number. Any number of the form $2^n + 1$ with $n = 2^t$. If the number is prime, it is called a Fermat prime. Define a number $F_n = 2^n + 1$. It may be shown that if n has an odd factor, then F_n is composite, but if $2^n + 1$ is prime, then n has *no* odd factors ($n = 2^t$ where t = any natural number). Thus, $n = 2^t$ is a necessary condition for $2^n + 1$ = prime.

If $n = ab$ and b is odd, then $2^a + 1$ is a factor of F_n. To ensure that b is odd, set $b = 2k + 1$. Then $F_n = 2^{(2k+1)a} + 1$. As before, one may show that $2^a + 1$ is a factor of F_n by constructing a trial case and then generalizing. Begin by choosing $k = 2$. Then, $F_n = 2^{5a} + 1$ and

$$\frac{2^{5a}+1}{2^a+1} = 2^{4a} - 2^{3a} + 2^{2a} - 2^a + 1 \qquad (6)$$

The division is exact. The trial case suggests the general solution:

$$\frac{2^{(2k+1)a}+1}{2^a+1} = 2^{2ka} - 2^{(2k-1)a} + 2^{(2k-2)a} - \ldots - 2^a + 1 \qquad (7)$$

which is also exact.

construction of regular polygon. Of n sides (using a compass and straightedge) possible if and only if

$$n = 2^a p_1 p_2 p_3 \ldots p_t \qquad (8)$$

where a = any natural number and $p_1, \ldots p_t$ are Fermat primes (Gauss).

Goldbach's conjecture. Unproved theorem that every even number ≥ 6 is the sum of two primes and every odd number ≥ 9 is the sum of three primes.

twin primes. Consecutive odd numbers that are both prime: (3,5), (5,7), (11,13). Mathematicians speculate but cannot prove that the number of such pairs is infinite.

Intervals of the Real Line

interval. A subset (neighborhood) of the real line containing all real numbers (points) between two given real numbers (a and b) called endpoints. A proper interval is any interval subset of the real line other than the real line itself.

interior points of an interval**.** Those points lying strictly between the endpoints of the interval.

closed interval $[a,b]$**.** The closed set $\{x|a \leq x \leq b\}$.

open interval (a,b)**.** The open set $\{x|a < x < b\}$.

half-open or ***half-closed interval*** $(a,b]$**.** The set $\{x|a < x \leq b\}$.

half-open or ***half-closed interval*** $[a,b)$**.** The set $\{x|a \leq x < b\}$.

unbounded interval. A half-closed interval $[a,\infty)$ or an open interval (a,∞). The interval $(-\infty,\infty)$ may be considered either open or closed.

partition of an interval $[a,b]$**.** A finite sequence of points $\{x_i\}$ such that $a = x_1 < x_2 < \ldots < x_n = b$.

completeness property of real numbers. A property which states that every nonempty set of real numbers is contained in a smallest closed interval of real numbers (table 1).

TABLE 1.—COMPLETENESS PROPERTY OF REAL NUMBERS

Set A	Smallest closed interval containing A
$\{a\}$	$[a,a]$
$(-a,b)$	$[-a,b]$
$(-a,b] \cup [c,d]$ $\quad (\ni -a < b < c < d)$	$[-a,d]$
{Integers > 0}	$[1,+\infty]$
{Rational numbers}	$[-\infty,+\infty]$
$\{1/n \mid n > 0\}$	$[0,1]$

disk. The extension of an interval to the Cartesian or complex plane. An *open* disk of radius ε centered at a point (s,t) is the set of points defined by the formula $(x - s)^2 + (y - t)^2 < \varepsilon$. A *closed* disk of radius ε centered at (s,t) is the set of points defined by $(x - s)^2 + (y - t)^2 \leq \varepsilon$.

ball. The extension of the disk to three-dimensional space. An *open* ball of radius ε centered at a point (s,t,u) is the set of points $(x - s)^2 + (y - t)^2 + (z - u)^2 < \varepsilon$. A *closed* ball of radius ε centered at a point (s,t,u) is the set of points $(x - s)^2 + (y - t)^2 + (z - u)^2 \leq \varepsilon$. The ball may be extended to higher dimensional spaces by analogy. Equivalently: A *closed* ball (closed disk) $B_\varepsilon s$ or $B(s,\varepsilon)$ in topology is a set of points whose distance from a given point s is less than or equal to a given constant ε. An *open* ball (open disk, neighborhood) $N_\varepsilon s$ or $N(s,\varepsilon)$ in topology is a set of points whose distance from a given point s is strictly less than a given constant ε. A closed ball is sometimes called a "sphere," although the term sphere may also refer only to the frontier of the ball.

Relations

relation R from the set S to the set T**.** A rule that associates elements of T with elements of S to form a set (or sets) of ordered pairs $\{(s,t) \mid s \in S \text{ and } t \in T\}$, which may be viewed as a subset of the Cartesian product $S \times T$ and represented as a relation from S to T denoted $R{:}S \rightarrow T$ or sRt. A relation from a set S to itself is called a relation *on* S. A relation on a set S is usually a *binary* relation on S, although the notion may be extended to involve more than two elements as in the relation aRb, $c \equiv$ "a is between b and c."

A binary relation R is

commutative or ***permutable.*** For any elements s and t if $sRt = tRs$.

associative. For any elements s, t, and u if $(sRt)Ru = sR(tRu)$.

A binary relation R^* is

distributive over another binary relation R **.** For any elements s, t, and u, if $sR^*(tRu) = (sR^*t)R(sR^*u)$.

A binary relation R is

transitive. For any elements s, t, and u if sRt and tRu imply sRu.

symmetric. For any elements s and t if sRt iff tRs.

antisymmetric. For any elements s and t if sRt and tRs iff $s = t$.

strict or ***proper.*** For any elements s and t if sRt iff $s \neq t$.

weak. For any elements s and t if sRt includes the possibility $s = t$.

compact on a set S**.** For any elements s and t in S, if whenever sRt, there is some element γ in S such that $sR\gamma$ and γRt; e.g., less than $<$ is compact on the rational numbers since for any pair of rationals s and t, there is another rational $\gamma = 1/2(s + t)$ such that $s < \gamma < t$.

domain of a relation R from S to T**.** The subset of S whose elements appear as first elements in the ordered pairs (s,t) of R; i.e., the domain of R is the set $D = \{s \in S \mid (s,t) \in R\}$.

co-domain of a relation R from S to T**.** The entire set T.

range of a relation R from S to T**.** The subset of T whose elements appear as second elements in the

ordered pairs (s,t) of R; i.e., the range of R is the set $R = \{t \in T | (s,t) \in R\}$.

inverse of a relation R from S to T**.** The set $R^{-1} = \{(t,s) | (s,t) \in R\}$.

converse of a relation R**.** Another relation R^* that holds between the elements of ordered pair (s,t) iff R holds between the elements in the ordered pair (t,s); e.g., for the domain of males, s is the father *ot* t iff t is the son of s.

connected relation**.** One in which either the relation or its converse holds between any two members of the domain; e.g., for the reals, either $a \geq b$ or $b \geq a$.

Equivalence

equivalence relation ~ on a set S**.** A binary relation that is reflexive, symmetric, and transitive. The elements in each ordered pair (s_1,s_2) of an equivalence relation are *equivalent*: $s_1 \sim s_2$.

equivalence class of an element s in S**.** The set of all other elements of S that are equivalent to it. If two equivalence classes have an element in common, the two classes as sets are equal. The collection of distinct equivalence classes having the property that every element of S belongs to exactly one of them is a *partition* or a *quotient* set of S denoted $S/\sim$.

Theorem: Given a partition of a set S, an equivalence relation on S can be obtained by defining s_1 equivalent to s_2 if s_1 and s_2 belong to the same subset in the partition. Conversely, from any equivalence relation on S, a partition of S may be obtained.

The following is an example of an equivalence relation: Let $S = I$ (the set of integers) and define a relation R on S with $P(s,t)$ = "s is congruent to t modulo 3;" i.e., $s - t = 3n$, where n = any integer (denoted "$s \approx t \bmod 3$"). The set of integers may be written in tabular form as

$$I = \{\ldots,-3,-2,-1,0,+1,+2,+3,\ldots\} \qquad (9)$$

The relation s ≈ t mod 3 partitions I into three sets:

$$I_1 = \{\ldots,-9,-6,-3,0,+3,+6,+9,\ldots\} \qquad (10a)$$

$$I_2 = \{\ldots,-8,-5,-2,+1,+4,+7,+10,\ldots\} \qquad (10b)$$

$$I_3 = \{\ldots,-7,-4,-1,+2,+5,+8,+11,\ldots\} \qquad (10c)$$

The relation R is seen to be an equivalence relation ~ since

$$s \approx s \bmod 3 \qquad (11a)$$

$$s \approx t \bmod 3 \quad \text{only if} \quad t \approx \bmod 3 \qquad (11b)$$

$$s \approx t \bmod 3 \quad \text{and} \quad t \approx v \bmod 3 \quad \text{only if } s \approx v \bmod 3 \qquad (11c)$$

The sets I_1, I_2, and I_3 are therefore equivalence classes (e.g., $[-2] = I_2$). The partition or quotient set $S/\sim$ may be denoted $\{I_1,I_2,I_3\}$.

Ordering

strict ordering**.** An ordering relation (such as <) that excludes the possibility of equality between pairs of elements.

weak ordering**.** An ordering relation (such as ≤) that permits the possibility of equality between pairs of elements.

total ordering**.** An ordering on a set such that every element is related to every other by the relation or its converse (i.e., a relation R such that sRt or tRs); e.g., the relation less than < is a total ordering on the reals.

dense ordering**.** An ordering on a set in which there exists between any two comparable elements of S another element of S; e.g., the rational numbers are dense since, for any rational numbers a and b, the rational number $1/2(a + b)$ lies between.

connected ordering**.** An ordering on a set in which every element is related to every other by the relation or its converse.

complete ordering**.** An ordering on a set in which some of the elements are related to others either by the ordering relation or its converse, whereas the remaining elements are not related either way (ambiguous usage).

partial ordering**.** An ordering on a set in which some of the elements are related to others either by the ordering relation or its converse, whereas the remaining elements are not related either way; e.g., the relation of set inclusion is a partial ordering:

$$\{2,3\} \subset \{1,2,3,4\} \quad \text{but} \quad \{2,3,4\} \not\subset \{1,2,3\}$$
$$\text{and} \quad \{1,2,3\} \not\subset \{2,3,4\} \qquad (12)$$

A partially ordered set is Dedekind complete if every subset has a supremum and an infimum; e.g., the reals are not complete, but the interval [0,1] is.

linear ordering. An ordering on a set in which some of the elements are related to others so that (1) every element is related to itself (*aRa*); (2) if any two elements share the ordering relation and its converse, then they are the same element (*aRb* and *bRa* $\Leftrightarrow$ *a* and *b* are the same element); (3) if any two elements share the ordering relation and one of them shares the relation with another, then the first also shares the relation with the other (*aRb* and *bRc* $\Rightarrow$ *aRc*); and (4) any two elements share the ordering relation in at least one direction (*aRb* or *bRa*). This complex definition is usually reduced to read: a *linear ordering* is any ordering on a set that is reflexive, antisymmetric, transitive, and connected (complete); e.g., the weak inequality $\leq$ on the set of integers is a linear ordering:

> ***reflexive.*** For any integer *a*, it is true that $a = a$.
> ***antisymmetric.*** For any integers *a* and *b*, it is true that $a \leq b$ and $b \leq a$ implies $a = b$.
> ***transitive.*** For any integers *a*, *b*, and *c*, it is true that $a \leq b$ and $b \leq c$ implies $a \leq c$.
> ***connected.*** For any integers *a* and *b*, either $a \leq b$ or $a \geq b$.

well-ordered set. A linearly ordered set in which every subset has a least element; e.g., the relation less than < is well ordered on the integers but not on the reals, since an open set has no least member.

inductive ordering. An ordering on a set such that every subset has at least one minimal element. A well-ordered set is inductively ordered.

For any ordered set, the element that is less than (or equal to) every other element in the set is the first or smallest element of the set. The element that is greater than (or equal to) every other element in the set is the last or largest element of the set. The first or smallest element precedes the other elements of the set. The last or largest element follows the other elements of the set.

An element in a set *S* is

> ***upper bound.*** If it follows every element of *S*. That element is a supremum or least upper bound if it is an upper bound and precedes every other upper bound of *S*.
> ***lower bound.*** If it precedes every element of *S*. That element is an infimum or greatest lower bound if it is a lower bound and follows every other lower bound of *S*. If *S* has an upper bound, it is bounded above. If *S* has a lower bound, it is bounded below. A set is bounded if it is bounded above and below. Any nonempty set that is bounded above has a supremum, and any nonempty set that is bounded below has an infimum. An unbounded set is any set that is not bounded.
> ***maximal.*** If it is followed by no other element than itself.
> ***minimal.*** If it is preceded by no other element than itself.

Minimal and maximal elements do not have to be the unique least or greatest element unless the ordering is total.

> ***maximum.*** If it is the largest element of the set; e.g., the negative numbers have no maximum, but the nonpositive numbers have a maximum 0. Both sets have 0 as a supremum.
> ***minimum.*** If it is the least element in the set; e.g., the positive numbers have no minimum, but the nonnegative numbers have a minimum 0. Both sets have 0 as an infimum.

closed interval [*s*,*t*]**.** An interval that has both a minimum and an infimum *s* and a maximum and a supremum *t* in the interval. The intervals $[s,\infty)$ and $(-\infty,s]$ may be regarded as closed.

open interval (*s*,*t*)**.** An interval that is bounded with infimum *s* and supremum *t*. The open interval is an open set. The intervals (x,∞) and $(-\infty,x)$ may be considered open intervals. The real line R^1 may also be considered an open interval.

half-open intervals [*s*,*t*) and (*s*,*t*]**.** Intervals that are bounded with an infimum *s* and a supremum *t* but only [*s*,*t*) has a minimum and (*s*,*t*] has a maximum. The half intervals are not open sets since neither

contains the neighborhood of the closed-end endpoint.

Mapping

mapping f from S to T where S and T are nonempty sets (or classes or spaces)**.** A rule that assigns to each element of S a unique element of T. A mapping is a specific type of relation R from S to T in which each element of S appears only once as a first element in the ordered pairs (s,t). The mapping f from S to T is denoted $f:S \to T$; if s is a member of S and $f(s)$ is the corresponding member of T, the mapping may be denoted $f:s \to f(s)$. The term $f(s)$ is called the image of s under f.

continuous mapping $f:S \to T$**.** One in which for any element t in T with open neighborhood V (arbitrarily small), there is a corresponding element s in S with open neighborhood U so that every element s^* in U is carried to an element t^* in V.

one-to-one or ***injective mapping*** $f:S \to T$**.** One that associates a unique member $f(s)$ in T with every member s of S.

onto or ***surjective mapping*** $f:S \to T$**.** One that associates with every element t of T at least one element of S such that $t = f(s)$.

bijective mapping $f:S \to T$**.** One that is both one to one and onto.

closed mapping $f:S \to T$**.** One that sends closed sets in S to closed sets in T.

***open mapping*.** One that sends open sets in S to open sets in T.

inverse mapping f^{-1} from T to S (also a bijection)**.** One for which an element t in T has a unique image $f^{-1}(t)$ in S. If $(s,f(s))$ belongs to f and $(f^{-1}(t),t)$ belongs to f^{-1}, then $(s,f(s)) = (f^{-1}(t),t)$.

restriction of mapping $f:S \to T$**.** Another mapping $g:S_1 \to T_1$, denoted $g = f|S_1$ where $S_1 \subseteq S$, $T_1 \subseteq T$, and $g(s_1) = f(s_1)$ for all s_1 in S_1.

equality of mappings $f:S \to T$ and $g:S \to T$**.** Two mappings that have the same domain S and $f(s) = g(s)$ for every s in S.

Two sets A and B are equivalent ($A \sim B$) if there exists a bijective mapping $f:A \to B$. A set is *infinite* if it is equivalent to a proper subset of itself; otherwise, it is *finite*.

graph of a mapping $f:S \to T$**.** The subset of ordered pairs $\{(s,f(s)) \in S \times T\}$. The graph of a mapping has the unique property that for each s in S, there is a unique element $(s,f(s))$ in the graph.

domain or ***essential domain*** of a mapping $f:S \to T$**.** The subset of S whose elements appear as first elements in the ordered pairs (s,t) of f; i.e., the domain of R is the set $D = \{s \in S | (s,f(s)) \in f\}$.

co-domain of a mapping $f:S \to T$**.** The entire set T.

range of a mapping $f:S \to T$**.** The subset of T consisting of just those elements $f(s)$ that are images of s in S under f; i.e., the range of f is the set $R = \{f(s) \in T | (s, f(s)) \in f\}$.

composition of two mappings $f:S \to T$ and $g: T \to U$**.** Another mapping $g\ f:S \to U$ defined by $(g \times f)(s) = g(f(s))$ for s in S. The mapping $g \times f:S \to U$ exists if and only if the co-domain of f equals the domain of g. The composition of mappings is *associative*; thus, if $f:S \to T$, $g:T \to U$, and $h:U \to V$ are mappings, then $h \times (g \times f) = (h \times g) \times f$ with domain S and co-domain V.

identity mapping on a set S**.** A mapping $i_S:S \to S$ defined by $i_S(s) = s$ for all s in S. Identity mappings have the property that if $f:S \to T$ is a mapping, then $f \times i_S = f$ and $i_T \times f = f$; e.g., the inverse mapping $f^{-1}: T \to S$ is a bijection with the property that $f \times f^{-1} = i_T$ and $f^{-1} \times f = i_S$.

Transformations

***transformation*.** A one-to-one mapping from S to S. If S is the set of points in the plane, then an important set of transformations in the plane is the linear transformations that (in Cartesian coordinates with origin O) can be represented by linear equations. Examples for a fixed origin O include rotations about O, reflections in lines through O, and dilatations from O. Translations are linear transformations in which O is not a fixed point.

***rotation*.** A transformation in which a coordinate system is turned in some direction around a fixed origin.

***reflection*.** A transformation in which the direction of one (or more) coordinate axis is reversed.

***dilatation*.** A transformation in which a coordinate system is stretched or shrunk around a fixed origin. Thus, a point x is mapped to a new point kx where

k is a scale factor. A dilatation is a direction preserving similarity.

translation. A transformation in which the origin of a coordinate system is moved from one position to another with the new axes parallel to the old.

affine transformation. A mapping that preserves co-linearity and, hence, parallelism and straightness, but may vary distances between points and angles between lines. Translation, rotation, and reflection in an axis are all affinities.

similarity transformation in Euclidean geometry**.** A mapping that preserves similarity and is some combination of a translation, a rotation, and/or a homothety.

homothety. A linear transformation that involves no rotation but does involve both a translation and a dilatation (i.e., is a composition of a translation and a dilatation).

similitude. A homothety that leaves the origin fixed. In vector terms, a similitude has the form $\mathbf{x} \rightarrow k\mathbf{x}$ where k is the ratio of similitude, and the origin is the center of similitude.

morphism. A transformation that preserves some structure on a set.

homomorphism. A mapping θ between two abstract algebras in which the structural properties of the domain are preserved in the range; i.e., if $*$ is the operation on the domain and $\times$ is the operation on the range, then $\theta\,(a * b) = \theta(a) \times \theta(b)$. Refer, also, to entry under Abstract Algebra.

monomorphism. An injective homomorphism.

epimorphism. A surjective homomorphism.

isomorphism. A bijective homomorphism; e.g,, the group of complex numbers $1, -1, i, -i$ is isomorphic to the group of elements 0, 1, 2, 3 with addition modulo 4.

automorphism. An isomorphism in which the domain and the range are identical; e.g., the permutations on a set are an automorphism.

deformation. A transformation whose effect is to change the shape of a figure by stretching but not tearing.

homotopy. A continuous deformation of one function or curve into another.

homeomorphism. A mapping between sets that is one to one and onto, so that both the function and its inverse are continuous. Homeomorphism is an equivalence relation that preserves topological properties; e.g., in the case of a geometric figure, a deformation is a homeomorphism.

isometry. An automorphism or a homeomorphism that preserves metric relations.

Functions

Real Functions

real function f. A mapping from the set R of real numbers (or a subset of R) to R. Thus, for every real number x in the domain, a real number $f(x)$ is defined. In analysis, a function $f{:}S \rightarrow R$ is often defined by giving a formula for $f(x)$ without specifying the domain S. In this case, it is usual to assume that the domain is the largest possible subset S of R. If the domain of a function f is R^n, then f is called a function *on* R^n. If the range of a function f is a subset of R^1, then the function is called a scalar-valued function. If the range of a function f is a subset of R^s where $s > 1$, then f is called a vector-valued function; e.g., $f(x,y,z) = (u,v)$ is a vector-valued function *on* R^3 with components u and v.

If a real function $f{:}S \rightarrow T$ is a bijection, then an inverse function f^{-1} from T to S may be defined as one for which an element y in T has a unique image $f^{-1}(y)$ in S. If $(x, f(x))$ belongs to f and $(f^{-1}(y),y)$ belongs to f^{-1}, then $(x,f(x)) = (f^{-1}(y),y)$. If the domain S is an interval I and f is strictly increasing or strictly decreasing on I, then an inverse function certainly exists. In general, when an inverse function is required for a given function f, it may be necessary to restrict the domain and obtain instead the inverse for this restriction of f. When the inverse function exists, the graphs of $y = f(x)$ and $x = f^{-1}(y)$ are reflections of one another in the line $y = x$.

The limit of a real function $f(x)$ as x tends to some value c in the domain is a number L, provided that $f(x)$ gets arbitrarily close to L when x gets arbitrarily close to c.

A real function $f(x)$ is *continuous*

at $x = c$. If and only if $f(c)$ exists and the limit of $f(x)$ as x approaches c is $f(c)$ (i.e., $\lim_{x \rightarrow c} f(x) = f(c)$).

in an open interval (a,b) ***with*** $a < b$**.** If it is continuous at every point in the interval.

on a closed interval $[a,b]$**.** If it is continuous on the open interval (a,b) and if the limit as x approaches a or b from within the interval equals $f(a)$ or $f(b)$, respectively (i.e., $\lim_{x\downarrow a} f(x) = f(a)$ or $\lim_{x\uparrow b} f(x) = f(b)$).

A real function is

increasing in or ***on an interval*** I**.** If $f(x_2) \geq f(x_1)$ whenever x_2 and x_1 are in I with $x_2 > x_1$. Also, f is strictly increasing if $f(x_2) > f(x_1)$ whenever $x_2 > x_1$.

decreasing in or ***on an interval*** I**.** If $f(x_2) \leq f(x_1)$ whenever x_2 and x_1 are in I with $x_2 > x_1$. Also, f is strictly decreasing if $f(x_2) < f(x_1)$ whenever $x_2 > x_1$.

monotonic over an interval I**.** If it is either increasing or decreasing on I. Also, a real function is strictly monotonic over an interval I if it is either strictly increasing or strictly decreasing on I.

bounded. If there is a number M such that for all numbers x in the domain of f, $|f(x)| < M$.

Theorem: If f is continuous on the closed interval $[a,b]$, then it is bounded on $[a,b]$.

Theorem: If f is continuous on the closed interval $[a,b]$, then there are numbers A and B such that $f([a,b]) = [A,B]$.

Algebraic Functions

algebraic function f**.** A mapping involving a finite number of algebraic operations ($\times$, /, +, −) from the complex domain C (or a subset of C) to C. Thus, for every complex number z in the complex plane, another complex number $f(z)$ is defined. Since $R^2 \subset C$, algebraic functions include mappings from and/or to R^2. Some examples of algebraic functions include

constant function. A real function f such that $f(z) = c_0$ for all z in C, where c_0, the value of f, is a fixed complex number.

linear function. A real function f such that $f(z) = az + b$ for all z in C, where a and b are real numbers with normally $a \neq 0$.

polynomial function. A real function f such that $f(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n$ for all z in C. The numbers $a_0,\ldots, a_n$ (with $a_n \neq 0$) are real number *coefficients*, and n is an integer equal to the *degree* of the polynomial.

rational function. A function f such that for z in the domain $f(z) = g(z)/h(z)$, where $g(z)$ and $h(z)$ are polynomials that may be assumed to have no common factor with degree greater then or equal to 1. The domain is usually taken to be the whole of C with any zeros of $h(z)$ omitted.

transcendental function. Any function of a complex variable that is not algebraic is transcendental. Algebraic functions correspond to classical geometric constructions that can be completed in a finite number of steps; transcendental functions correspond to classical geometrical constructions that require an infinite number of steps to complete, such as, for example, obtaining a circle by repeatedly subdividing the sides of a polygon. Solutions to transcendental equations involve transcendental numbers. Examples of transcendental functions include infinite series and such defined functions as $\log(x)$, $\sin(x)$, e^x.

Set Functions

set function. A mapping from one class S of sets onto another class T of sets. Thus, a set function is any function whose domain consists of sets and whose co-domain also consists of sets.

real-valued set function. A set function whose domain consists of sets and whose co-domain consists of the set of real numbers.

characteristic function of a set S in some universe of discourse U. The real-valued function $f_S: U \rightarrow \{1,0\}$ defined by $f_S(s) = 1$ if s is an element of S and $f_S(s) = 0$ if s is not an element of S.

choice function of a set S**.** A function that maps any class of nonempty subsets of S into S in such a way that the image of each subset in S is an element of that subset.

Sequences

sequence. A set of terms $\{a_1,a_2,a_3,\ldots\}$ that are functions from the integers (or some subset of the

integers) to the real numbers. The terms of the sequence may be represented as ordered pairs $\{(1,a_1), (2,a_2), (3,a_3),\ldots\}$, emphasizing the functional relationship. Because the terms are paired with the integers 1, 2, 3,…, one may speak of the first term a_1, the second term a_2, and so on. The terms of a sequence need not be distinct; e.g., let $\{a_n\}$ with $n > 0$ be the sequence {1,1,1,0,1,0 1,…} in which $a_n = 1$ if n is prime (or 1) and 0 otherwise.

finite sequence. One that consists of a finite number of terms $\{a_1,a_2,a_3,\ldots,a_n\}$, where n is the length of the sequence.

infinite sequence. One that consists of a denumerable infinity of terms $\{a_1,a_2,a_3,\ldots\}$ corresponding to each of the positive integers.

monotonic sequence $\{a_1,a_2,a_3,\ldots\}$**.** One that is either increasing ($a_n \leq a_{n+1}$ for all n) or decreasing ($a_n \geq a_{n+1}$ for all n).

strictly monotonic sequence. One that is either strictly increasing ($a_n < a_{n+1}$ for all n) or strictly decreasing ($a_n > a_{n+1}$ for all n).

bounded sequence $\{a_1,a_2,a_3,\ldots\}$**.** A sequence for which there is a number $M > 0$ such that for all n, $|a_n| < M$.

A sequence may be defined by any rule that assigns a real number a_n to a positive integer n:

recursion formula. Defines by specifying the first term and then stating a recursion formula that tells how to find each remaining term from the term that precedes it; e.g., let $\{a_n\}$ be the sequence in which $a_1 = 1$ and $a_n = 3a_{n-1} - 1$ for $n > 1$.

arithmetic formula. Defines by specifying an arithmetic formula for the general term a_n; e.g., let $\{a_n\}$ be the sequence in which $a_n = 2^n + 1$ for $n > 0$.

inference from given terms. Defines by specifying a sufficient number of initial terms from which the general pattern may be inferred; e.g., let $\{a_n\}$ be the sequence $\{1,1/2,1/3,1/4,1/5,\ldots\}$.

random sequence. A sequence that exhibits no apparent rule (no matter how many terms are considered) for which the next cannot be predicted with certainty.

doubling sequence. A sequence such as {1,2,4,8,16,…} for which the first term is 1 and for which $a_{n+1} = 2a_n$.

Fibonacci sequence. A recursive sequence {1,1,2,3,5,8,13,21,…} where starting with the first two terms as 1,1, each new term is made by adding the previous two terms.

Lucas sequence. Another recursive sequence {1,3,4,7,11,18,…} where starting with the first two terms as 1,3, each new term is made by adding the previous two terms.

arithmetic progression. Any sequence in which the difference ($a_{n+1} - a_n$) between successive terms is a constant.

geometric progression. Any sequence in which the ratio (a_{n+1}/a_n) between successive terms is a constant.

The limit of an infinite sequence $\{a_1,a_2,a_3,\ldots\}$ is a number L provided that a_n becomes arbitrarily close to L as n approaches infinity. The usual notation is $\lim_{n\uparrow\infty} a_n = L$ or simply $a_n \to L$; e.g., the sequence {0,1/2,3/4,15/16,…} has the limit $a_n \to 1$.

Sequences that have no limit may be classified as

1. $a_n \to \infty$, for any positive number K (however large), if there is an integer S (which depends on K) such that for all $n > S$, $a_n > K$; e.g., the sequence {0,1,4,9,16,…} has the limit $a_n \to \infty$.
2. $a_n \to -\infty$, for any negative number K (however small), if there is an integer S (which depends on K) such that for all $n > S$, $a_n < K$.
3. A sequence that does not have a limit but is bounded is said to *oscillate finitely*; e.g., the sequence {1/2,–3/4,4/5,–5/6…} oscillates finitely.
4. A sequence that is not bounded and for which it is not the case that $a_n \to \pm\infty$ is said to oscillate infinitely; e.g., the sequence {1,2,1,4,1,8,1,16,…} oscillates infinitely.

convergent sequence. One that has a limit; e.g., an unending decimal is a convergent sequence. Consider the fraction 25/33 = 0.7575757575… This decimal corresponds to the sequence {0.7,0.75,0.757,0.7575,0.75757,…} that converges to 25/33 in the limit as n approaches infinity.

infinite sequence $\{a_1,a_2,a_3,\ldots\}$**.** One that has a limit if the difference $a_{n+k} - a_n$ approaches zero as n and k independently approach infinity. Any sequence that has this property is called a Cauchy sequence or a fundamental sequence. Notice that Cauchy's condition makes no reference to the value of the limit itself.

Theorem: If a sequence converges, it is bounded (or if a sequence is not bounded, it does not converge).

Theorem: A monotonic sequence converges if and only if it is bounded. The limit of an increasing sequence is its least upper bound, and the limit of a decreasing sequence is its greatest lower bound.

divergent sequence. A sequence that does not converge.

accumulation point of a sequence**.** Any point P where there is an infinite number of terms in any neighborhood of P; e.g., the sequence $\{1,1/2,1,1/3,1,1/4,1,1/5,\ldots\}$ has two accumulation points: one at 1 and the other at 0. Every bounded infinite sequence of real numbers contains at least one accumulation point.

For real number sequences, the largest accumulation point is called the *limit superior*, and the smallest accumulation point is called the *limit inferior*. The limit superior and limit inferior do not necessarily correspond to least upper and greatest lower bounds of the sequence; e.g., the limit superior and limit inferior of the sequence $\{2,-3/2,4/3,-5/4,6/5,-7/6,\ldots\}$ are +1 and −1, respectively, whereas the upper and lower bounds are 2 and −3/2, respectively. The limit superior and limit inferior of any sequence $\{a_n\}$ are denoted respectively by $\lim_{n\to\infty}\sup a_n$ and $\lim_{n\to\infty}\inf a_n$. When these two limits are the same, the sequence has a limit.

nested sequence of intervals $I_1,I_2,I_3,\ldots,I_n,\ldots$ A sequence of intervals in which each is contained in the preceding: $I_1 \supset I_2 \supset I_3 \supset\ldots \supset I_n \supset\ldots$ It is sometimes required that the lengths of the intervals approach zero as n approaches infinity.

For any sequence of nested intervals, each of which is bounded and closed, there is at least one point that belongs to all the intervals.

A collection of sets is nested if for any two members, one is contained in the other. A nested collection of sets is also called a nest, a tower, or a chain.

Theorem: In a complete metric space, any nested sequence of sets whose diameters tend to zero contains a unique point of intersection.

Curves, Surfaces, and Regions

curve (or ***path***) between two points**.** A continuous deformation f of the closed interval [0,1] in which the images of the endpoints $f(0)$ and $f(1)$ are the two given points.

closed curve. One that has no endpoints and completely encloses a finite area. It is a continuous deformation f of the closed interval [0,1] for which $f(0) = f(1)$. A closed curve is simple if it does not intersect with itself.

The *Jordan Curve Theorem* states that any simple closed curve has an interior and an exterior; i.e., the plane is divisible into two, open, disjoint regions, each with the curve as its closure.

bounded surface without holes. A continuous deformation of the closed unit disk $(x - s)^2 + (y - t)^2 \le 1$ in which the boundary of the surface is the image of the unit circle $(x - s)^2 + (y - t)^2 = 1$. A bounded surface with m holes is a continuous deformation of the closed unit disk with m open regions removed from its interior.

A bounded surface is *simply connected* if every simple closed curve drawn on it may be continuously contracted to a point without leaving the surface. A bounded surface is n-tuply connected if it has $m = n - 1$ holes or, equivalently, if at most $n - 1$ cuts are required to make it homeomorphic to a closed unit disk.

closed surface without holes. One that has no boundary and completely encloses a finite volume. It is a continuous deformation of the closed unit disk for which the disk boundary is mapped into a single point of the surface. A closed surface with m holes is

a continuous deformation of the closed unit disk with m open regions removed from its interior.

A closed surface is *simply connected* if every simple closed curve drawn on it may be continuously contracted to a point without leaving the surface; e.g., a disk and a sphere are simply connected, but an annulus is not. A closed surface is n-tuply connected if at most $n - 1$ cuts may be made in it without dividing it into two parts.

A region in three-space, bounded by a surface, is a continuous deformation of the closed unit ball $(x - s)^2 + (y - t)^2 + (z - u)^2 \leq 1$, in which the surface is the image of the unit sphere $(x - s)^2 + (y - t)^2 + (z - u)^2 = 1$.

A region in three-space is simply connected if every closed curve in the region bounds a surface that is simply connected; e.g., the interior of a sphere is simply connected, but the interior of a torus is not.

The *Jordan-Brouwer Separation Theorem* proves that a topological $(n - 1)$-sphere separates n-dimensional Euclidean space into two open, disjoint parts, each with the $(n - 1)$-sphere as its closure.

Mathematical Spaces

point. Any element in a metric space, a Euclidean space, a topological space, or a vector space.

real line. An infinite line on which points are taken to represent the real numbers by their distance from a fixed origin.

mathematical space. A set of elements, called points, endowed with a structure defined by specifying a set of axioms to be satisfied by the elements; e.g., metric space, vector space, normed space, Euclidean space, n-space, topological space. A subspace is any subset of a space that is itself a space, esp. one that has the essential properties of the including space.

metric space. A set S in which for all pairs of elements a and b, there is a nonnegative real number M (distance from a to b) that satisfies the following conditions: $M = 0$ if a and b are the same point; M from a to b equals M from b to a; and for c also in S, M from a to b plus M from b to c is greater than or equal to M from a to c (triangle inequality). Any function M that satisfies these conditions is called a metric for S.

open set S in a metric space**.** One in which every point has an open neighborhood lying entirely within S; i.e., each point of S is an interior point. Equivalently, an open set in a metric space is a set in which every point is in an open ball lying within the set. An open set is the complement of a closed set. Note: The null set Φ is an open set since there is no point in the empty set that is not an interior point: *On the real number line the open interval (a,b), where a and b are real numbers, is an open set in* R^1. *In the plane, the open disk with center at* (α,β) *and radius* $\delta > 0$ *defined by* $(x - \alpha)^2 + (y - \beta)^2 < \delta^2$ *is an open set in* R^2.

open neighborhood (or simply, a neighborhood) $N(\varepsilon,s)$ of a point s in a metric space S**.** The set of all points whose distance from s is strictly less than some arbitrarily small value ε, called the "radius." An open neighborhood is also called an open ball or open sphere.

closed neighborhood of a point s in S**.** The set of all points whose distance from s is less than or equal to ε.

punctured neighborhood of a point s in S**.** A neighborhood from which the point s itself has been deleted; i.e., a punctured neighborhood of s is the set difference $N(\varepsilon,s)\backslash\{s\}$.

vector space. A set S, which is an *Abelian group* (defined over a field F) together with their individual associated operations. The elements s in S are referred to as "vectors," and the elements ϕ in F are referred to as "scalars." Another operation is defined so that the product of a vector and a scalar is another vector. This operation distributes over the addition of both scalars and vectors and is associative with the multiplication of scalars. In analysis, the field F is usually the set of real or complex numbers.

normed space. A vector space endowed with a norm. A norm is the length of a vector, a nonnegative real number, independent of the sense of the vector, defined so that for some scalar ϕ in the field F, the norm of the product of ϕ and a vector is the product of $|\phi|$ and the norm of the vector. For two vectors, the norm of their [vector] sum is less than or equal to the sum of their norms. In a *Hilbert space*, an inner product between vectors is defined so that the inner

product of a vector with itself is the square of the norm of that vector.

Euclidean space. Any finite dimensional vector space possessing an inner product so that a Euclidean distance may be imposed. An *n*-dimensional Euclidean space may be generated as the *n*-fold Cartesian product of the real or complex fields. More generally, a Euclidean space is any finite or infinite dimensional inner product space.

n-space. Any mathematical space with *n*-dimensions; a mathematical space in which *n*-independent coordinates are required to locate a point in the space.

topological space. Any set *S* in which a class of open subsets has been chosen having the properties that the class includes, as two of its members, both the empty set and the set *S* itself and is closed under the operations of set union and set intersection.

A topological space is

- ***connected.*** If it cannot be partitioned into two nonempty open subsets, each of which has no points in common with the closure of the other. The rationals are not connected, although the reals are.
- ***separated.*** If for two open sets in the space, neither intersects the closure of the other. A topological space is connected if and only if it cannot be written as the union of two nonempty separated sets.
- ***compact.*** If every sequence in the space contains a subsequence that converges to a point in the space. Thus, the interval [0,1] on the real line is compact, whereas the interval (0,1) is not. The subsequence 1/2,1/3,1/4, 1/5,… converges to 0, which is a member of [0,1] but is not a member of (0,1).

Theorem: A subset of a Euclidean space is bounded and closed if and only if it is compact.

manifold. An *n*-dimensional topological space that is locally Euclidean; a space in which for every point, there is a neighborhood that is homeomorphic to the interior of a sphere in Euclidean *n*-space.

affine manifold. A vector subspace that permits affine transformations. A nontrivial affine manifold in three-space must be a point, a line, or a plane.

Abstract Algebra

operation on a set *S.* A rule that associates with some number of elements of *S* a resulting element. An operation that associates with one element of *S* a resulting element is called a *unary* operation; one that associates with two elements of *S* a resulting element is called a *binary* operation: *Logical negation is a unary operation; addition and multiplication are binary operations.*

A set *S* is

- ***open*** under an operation**.** If it fails to contain all the members of the set *S** produced by the operation acting on its members; e.g., the integers are closed under addition and subtraction but not under division, since for any positive integer *m*, *m*/0 is not an integer (*m*/0 is undefined).
- ***closed*** under an operation**.** If it contains all the members of the set *S** produced by the operation acting on its members; e.g., the positive integers are closed under addition but not under subtraction, since for any positive integers m and n with $m \neq n$, $(n + m)$ is a positive integer, but either $(m - n)$ or $(n - m)$ is not.

closure of a set under an operation**.** The smallest closed set containing the given set and all the elements produced by the operation acting upon the set; e.g., the closure of the positive integers under the operation subtraction is the set of all integers.

algebraic closure of a set**.** The extension of a given set or field to one that contains all the roots of all the polynomials whose coefficients are members of the given set. A set is algebraically closed if it coincides with its algebraic closure: *Neither the rationals nor the reals are algebraically closed since they do not contain roots of the polynomial* $x^2 + 1 = 0$. *The complex field is algebraically closed and is the closure of both subfields.*

group. Any set *S* that is closed under a binary associative operation $\oplus$ in which there is an identity element $e_\oplus$ such that for any a in *S*, $a \oplus e_\oplus = e_\oplus \oplus a = a$ and in which for any a in *S*, there is an inverse element a^{-1} in *S* such that $a \oplus a^{-1} = a^{-1} \oplus a = e_\oplus$: *The integers are a group under addition but not under multiplication*. If all the elements of the set

are commutative under $\oplus$, then the group is a commutative or Abelian group; e.g., all cyclic groups, such as integers under addition modulo n, are Abelian. A subgroup is any subset of a group that is itself a group relative to the same operation: *The integers are a subgroup of the reals under addition, but the integers modulo n is not, since addition modulo n is differently defined*.

Summary of Group Operations

If S is a group and $a,b,c \in S$, then

1. $a \oplus b \in S$
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. $\forall\ a \in S, \exists\ e_{\oplus} \in S \ni a \oplus e_{\oplus} = e_{\oplus} \oplus a = a$ (identity element)
4. $\forall\ a \in S, \exists\ (-a) \in S \ni a \oplus (-a) = (-a) \oplus a = e_{\oplus}$ (inverse element)

also

5. $\forall\ a,b \in S, a \oplus b = b \oplus a \Rightarrow S$ is a commutative group

topological group. An abstract group (also a topological space) with continuous group operations. Continuous group operations means that if a and $b \in S$, then

1. $\forall$ neighborhoods W of $a \oplus b$, $\exists$ individual neighborhoods U and V of a and $b \ni \forall\ u \in U$ and $v \in V, u \oplus v \in W$
2. $\forall$ neighborhoods V of a^{-1}, $\exists$ neighborhoods U of $a \ni \forall\ u \in U, u^{-1} \in V$

The set of all real numbers is a topological group.

ring. Any set S that is closed under two binary operations ($\oplus$ and $\otimes$), of which $\oplus$ forms a *commutative* group with the set and $\otimes$ is *associative* over the set and *distributive* with respect to $\oplus$.

commutative ring. A ring whose elements are also commutative under $\otimes$; the even integers form a commutative ring.

commutative ring with identity. A ring possessing an identity element $e_{\otimes}$ (in S) such that for any a in S, $a \otimes e_{\otimes} = e_{\otimes} \otimes a = a$, then the ring is a commutative ring with identity; the integers are a commutative ring with identity, but the even integers are not.

subring. Any subset of a ring that is itself a ring relative to the same operations: The set of integers is a subring of the real numbers, and the set of all even integers is a subring of the integers.

Summary of Ring Operations

If S is a ring and $a,b,c \in S$, then

1. $a \oplus b \in S$
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. $\forall\ a \in S, \exists\ e_{\oplus} \in S \ni a \oplus e_{\oplus} = e_{\oplus} + a = a$ (identity element for $\oplus$)
4. $\forall\ a \in S, \exists\ (-a) \in S \ni a \oplus (-a) = (-a) \oplus a = e_{\oplus}$ (inverse element for $\oplus$)
5. $\forall\ a,b \in S, a \oplus b = b \oplus a$
6. $a \otimes b \in S$
7. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
8. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
9. $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$

also

10. $[\forall\ a,b \in S,\ a \otimes b = b \otimes a] \Rightarrow S$ is a commutative ring

and

11. $[\forall\ a \in S\ \exists\ e_{\otimes} \in S \ni a \otimes e_{\otimes} = e_{\otimes} \otimes a = a] \Rightarrow S$ is a commutative ring with identity

zero ring. A commutative ring with identity consisting of only a single element 0 with multiplication and addition defined by $0 \oplus 0 = 0 = 0 \otimes 0$.

module M over a ring R (also R-module)**.** A commutative group endowed with an exterior multiplication (either on the left or on the right) that is associative and distributive and multiplies group elements by ring elements (called "scalars") to produce group elements. Every commutative group may be viewed as a module over the integers. A vector space is a module in which R is a field. Every ring R may be viewed as an R-module over itself, and an ideal in R is an R-module.

homomorphism θ**.** A mapping from one algebraic structure to another under which the structural properties of the domain are preserved in the range: if $*$ is the operation on the domain, and $\times$ is the operation on the range, then $\theta(s * t) = \theta(s) \times \theta(t)$.

***group homomorphism*.** A mapping θ such that both the domain and the range are groups, and $\theta(st) = \theta(s)\theta(t)$ for all s and t in the domain.

***ring homomorphism*.** A mapping θ from one ring to another such that $\theta(s + t) = \theta(s) + \theta(t)$ and $\theta(st) = \theta(s)\theta(t)$ for all s and t in the domain.

***module homomorphism*.** A mapping such that $\theta(s + t) = \theta(s) + \theta(t)$ and $\theta(\rho s) = \rho\theta(s)$ for all s and t in the R-module and ρ in the ring R. If R is a field, then θ is a linear mapping.

In group theory, homomorphisms are *surjective* unless otherwise noted.

***integral domain*.** A set S that is a commutative ring with multiplicative identity and contains no pair of elements whose product is $e_\oplus$ unless either $a = e_\oplus$, $b = e_\oplus$, or both. Thus, for any a and b in S, $a \otimes b = b \otimes a = e_\oplus$ implies that either $a = e_\oplus$, $b = e_\oplus$, or $a = b = e_\oplus$; e.g., the integers under the operations of addition and multiplication are an integral domain, as are the integers modulo n, provided that n is prime.

Equivalent definition: An integral domain is a commutative ring that contains no proper divisor equal to $e_\oplus$. Thus, $a = b$ whenever $a \otimes c = b \otimes c$ and $c \neq e_\oplus$.

Summary of Integral Domain Operations

If S is an integral domain, then in addition to conditions 1 to 11 above, the following condition must be added:

$$12.\ [\forall\ a,b \in S,\ a \otimes b = 0] \Rightarrow (a = 0) \vee (b = 0)$$

***field*.** A set S that is an integral domain with a multiplicative inverse for every element. Thus, for every a in S, there is an a^{-1} in S such that $a \otimes a^{-1} = a^{-1} \otimes a = e_\otimes$; e.g., the rationals and the reals are fields, but the integers are not.

***subfield*.** A subset of a field that itself forms a field relative to the same operations.

Summary of Field Operations

If S is a field, then, in addition to conditions 1 to 12 above, the following condition must be added:

$$13.\ \forall\ a\ (\neq 0) \in S\ \exists\ a^{-1}\ \ni\ a \otimes a^{-1} = a^{-1} \otimes a = e_\otimes$$

topology τ **on a set** S**.** Any class of open subsets of S closed under the set operations of union and intersection. The choice of subsets in a given topology is not unique; many different topologies are possible.

***finer and coarser topologies*.** A topology τ_2 that is *finer* (larger) than another topology τ_1 if τ_2 strictly contains τ_1. Conversely, τ_1 is said to be *coarser* (smaller) than τ_2.

***discrete topology*.** A topology that consists of the entire power set.

***indiscrete topology*.** A topology that consists only of the empty set and the original set S itself.

***finest and coarsest topologies*.** On any given set, the topology that is discrete is the finest topology, and the topology that is indiscrete is the coarsest.

***comparable topologies*.** When one of two topologies on a set is finer than the other; conversely, if neither is finer than the other, they are not comparable.

usual topology on R^1**.** A topology formed on R^1 by the set of all open intervals on the real line R^1, along with R^1 itself and the empty set Φ.

usual topology on R^2**.** A topology formed on R^2 by the set of all open disks in the plane R^2, along with R^2 itself and the empty set Φ.

***topological space*.** A set S with a topology τ defined on it. A topological space is denoted $X = (S,\tau)$, and the members of τ are referred to as "τ-open sets" or "open sets." Let the set $S = \{a,b,c,d\}$ with $\tau_1 = \{\{a,b,c,d\}, \{a,b\}, \{c,d\}, \{\Phi\}\}$, and $\tau_2 = \{\{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}, \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\}, \{\Phi\}\}$ (the power set of S). Then $\tau_2 \supset \tau_1$ and is therefore a finer topology on S than τ_1.

Appendix A

Ideas From Various Mathematical Disciplines

Archimede's Axiom

Archimede's axiom. That if x is any real number, then there exists an integer n such that $n > x$.

Remark: Archimede's axiom is an ordering principle on the real numbers. It asserts that for any real number, it is possible to find a next larger integer.

Euclid's Axioms in Classical Geometry

Euclid's axioms

1. A straight line may be drawn from any point to any other point.
2. A finite straight line may be extended continuously in a straight line.
3. A circle may be described with any center and any radius.
4. All right angles are equal to one another.
5. If a straight line meets two other straight lines so as to make the sum of the two interior angles on one side of the transversal less than two right angles, the two other straight lines, extended indefinitely, will meet on that side of the transversal.

Equivalently, the fifth axiom may be replaced by *Playfair's axiom*:

5(a). Through a point not on a given line, there is one and only one parallel to the given line.

Remark: The fifth axiom was regarded as self-evident until the 19th century when non-Euclidean geometries were devised, retaining the first four of Euclid's axioms but not the fifth, which was omitted in favor of other possibilities (esp., in elliptic geometry, "Through a point outside a given line, there are no parallels to the given line." or in hyperbolic geometry, "Through a point outside a given line, there are at least two parallels to the given line."). Since the non-Euclidean geometries are consistent, the fifth axiom of Euclid must be independent of the other four.

Euclid's Prime Number Proof

Euclid's prime number proof. Demonstrates the infinity of primes: let $p_1, p_2, \ldots, p_n$ be any finite list of primes. Form the number $N = 1 + p_1 p_2 \ldots p_n$. N is not divisible by any of the primes $p_1, p_2, \ldots, p_n$ in the list, for the remainder 1 is always left over. Also, N is obviously greater than 1 and must be either prime itself or divisible by a prime not in the given list. Either way, there exists yet another prime that is not in the original list; therefore, the set of primes cannot be contained in any finite list.

Peano's Axioms in Number Theory

Peano's axioms

1. 0 is a natural number.
2. Every number x has another natural number as its successor (often denoted $S(x)$ or x').
3. For all x, $0 \neq S(x)$.
4. If $S(x) = S(y)$, then $x = y$.
5. If $P(n)$ is a proposition associated with each number n, $P(1)$ is true and for all k, $P(k)$ implies $P(k+1)$ is true, then $P(n)$ is true for all numbers.

Remark: This last axiom is known as the principle of induction. $P(1)$ is the base clause, and $P(k)$ implies that $P(k+1)$ is the recursion clause. Induction may be used to prove such statements as the sum of the first n natural numbers $\Sigma_n = 1 + 2 + \ldots + n = 1/2\ n(n+1)$. The base clause is obviously true for $n = 1$. The recursion clause requires that one show $\Sigma_{n+1} = 1 + 2 + \ldots + n + (n+1) = \Sigma_n + (n+1)$. By hypothesis, $\Sigma_n = 1/2\ n(n+1)$, so that $\Sigma_n + (n+1) = 1/2\ n(n+1) + (n+1) = 1/2\ (n+1)(n+2)$.

Goldbach's Conjecture in Number Theory

Goldbach's conjecture. That every even number greater than or equal to 6 may be represented as the sum of two odd primes.

Remark: Goldbach also conjectured that all odd numbers are the sum of three odd primes. Vinogradov's theorem shows that this conjecture is true of all but a finite number of odds.

Fermat's Last Theorem in Number Theory

Fermat's last theorem. That the equation $x^n + y^n = z^n$ has no solutions in whole numbers for x, y, and z if n is greater than 2, and $x, y, z > 1$.

Axiom of Choice in Set Theory

axiom of choice. That for any set S, there is a function (choice or selection function) f such that for any nonempty subset X of S, $f(X) \in X$.

Remark: The set of values of f is called a choice set. A choice function for S may be regarded as selecting a member from each nonempty subset of S; e.g., if $S = \{1,2\}$, the nonempty subsets of S are $X_1 = \{1\}$, $X_2 = \{2\}$, $X_3 = \{1,2\}$. The choice functions for S may then be defined: $f_1(X_1) = 1$, $f_1(X_2) = 2$, $f_1(X_3) = 1$, $f_2(X_1) = 1$, $f_2(X_2) = 2$, and $f_2(X_3) = 2$. Zermelo used this axiom to prove that every ordered set can be well ordered.

Fundamental Theorems of Mathematics

fundamental theorem of arithmetic. That every positive integer has a unique canonical (simplest form) decomposition as a product of its prime factors.

fundamental theorem of algebra. That a complex polynomial of degree n has precisely n complex roots, counting multiplicity. Therefore, the complex numbers are algebraically closed; i.e., the roots of all polynomials with complex coefficients are included in the set of complex numbers; the reals and the rationals are not algebraically closed since neither set contains the roots of $x^2 + 1 = 0$.

fundamental theorem of calculus. That if the derivative $f(x)$ of $F(x)$ is integrable (or if the function $F(x)$ is continuously differentiable) so that $F(x)$ is an indefinite integral of $f(x)$, then $\int_a^b f(x)dx = F(b) - F(a)$. Conversely, if $F(x)$ is defined as the integral of $f(x)$ from a to x for all x in $[a,b]$, then $f(x)$ is the derivative of $F(x)$ at every point of the interval at which $f(x)$ is continuous.

fundamental theorem of projective geometry. That three distinct, corresponding pairs of points uniquely determine a projectivity (projective transformation).

fundamental theorem of space curves. That the Frenet formulas for a space curve which recaptures the unit tangent T, normal N, and binormal B from the curvature κ and the torsion τ of the curve are

$$\frac{dN}{ds} = -\kappa T + \tau B, \qquad \frac{dB}{ds} = -\tau N,$$

and

$$\frac{dT}{ds} = \kappa N \quad (13)$$

where s is the arc length.

Gödel's proof. That any formal arithmetical system is incomplete in the sense that, given any consistent set of arithmetic axioms, there are true statements in the resulting arithmetical system which cannot be derived from these axioms.

Cantor's diagonal theorem. That the elements of the power set of any given set S, finite or infinite, cannot be put into one-to-one correspondence with the elements of S itself without remainder elements; i.e., any set has more subsets than it has elements.

diagonal process. The construction of a new member of a set S from a list of the given members of S by making the n^{th} term of the new member differ from the n^{th} term of the n^{th} element in the list. The new member is therefore distinct from every member in the list. The set that contains the new member must have a cardinality strictly larger than that of the original set S. The diagonal process was used by Cantor to prove the diagonal theorem and to show the uncountability of any proper interval on the real line.

Cardinal Arithmetic

Let σ and τ be the cardinal numbers of disjoint sets S and T, respectively. Then $\sigma + \tau$ is the cardinal number of $S \cup T$ and $\sigma\tau$ is the cardinal number of $S \times T$.

Theorem: The operations of addition and multiplication of cardinal numbers are associative and commutative, and addition distributes over multiplication. For cardinal numbers σ, τ, and γ,

Associative: $(\sigma + \tau) + \gamma = \sigma + (\tau + \gamma)$ and $(\sigma\tau)\gamma = \sigma(\tau\gamma)$

Commutative: $\sigma + \tau = \tau + \sigma$ and $\sigma\tau = \tau\sigma$
Distributive: $\sigma(\tau + \gamma) = \sigma\tau + \sigma\gamma$

The *difference* between two numbers σ and τ may be defined in terms of their sum in cardinal arithmetic. A number δ is the difference between σ and τ iff σ is the sum of τ and δ: $\sigma - \tau = \delta \Leftrightarrow \sigma = \tau + \delta$.

The *quotient* between two numbers σ and τ may be defined in terms of their product in cardinal arithmetic. A number δ is the quotient of σ and τ iff σ is the product of τ and δ: $\sigma/\tau = \delta \Leftrightarrow \sigma = \tau\delta$.

Appendix B

Divisibility of Integers in Base 10 (Integer$_{10}$)

Any integer represented in base 10 has the general form $I = a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots$where the a_i are themselves integers and are members of the set $\{0, \pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9\}$. Thus, $|a_i| \leq 9$.

An integer I_1 is *divisible* by another integer I_2 if there is an integer λ such that $I_1 = \lambda I_2$. I_2 is called a "divisor" or "factor" of I_1 and I_1 is called a "multiple" of I_2. The number λ is called a "quotient."

Divisibility by 2

Every even number is divisible by 2 since every even integer I_{even} has the form $I_{\text{even}} = 2k$ where k is itself *any* integer.

Divisibility by 3

Any integer for which the sum $a_0 + a_1 + a_2 + a_3 + \ldots$is divisible by 3 is itself divisible by 3 since

$$\begin{aligned} I &= a_0 + 10a_1 + 100a2 + 1000a3 + \ldots \\ &= a_0 + (9+1)a_1 + (99+1)a_2 + (999+1)a_3 + \ldots \\ &= (a_0 + a_1 + a_2 + a_3 + \ldots) + 9a_1 + 99a_2 + 999a_{3+\ldots} \end{aligned}$$

and

$$9a_1 + 99a_2 + 999a_3 + \ldots \qquad (14)$$

is already divisible by 3.

Divisibility by 4

Any integer for which $a_0 + 10a_1$ is divisible by 4 is itself divisible by 4 since

$$I = a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots$$

and

$$100a_2 + 1000a_3 + \ldots \qquad (15)$$

is already divisible by 4.

Divisibility by 5

Any integer for which a_0 equals ±1 or ±5 is itself divisible by 5 since

$$I = a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots \left|a_0\right| \leq 9$$

and

$$10a_1 + 100a_2 + 1000a_3 + \ldots \qquad (16)$$

is already divisible by 5.

Divisibility by 6

Any integer that is evenly divisible by 2 and by 3 is itself divisible by 6 since $(1/6)I = (1/2)(1/3)I$.

Divisibility by 8

Any integer for which $a_0 + 10a_1 + 100a_2$ is divisible by 8 is itself divisible by 8 since

$$I = a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots$$

and

$$1000a_3 + \ldots \qquad (17)$$

is already divisible by 8.

Divisibility by 9

Any integer for which the sum $a_0 + a_1 + a_2 + a_3 + \ldots$is divisible by 9 is itself divisible by 9 since

$$\begin{aligned} I &= a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots \\ &= a_0 + (9+1)a_1 + (99+1)a_2 + (999+1)a_3 + \ldots \\ &= (a_0 + a_1 + a_2 + a_3 + \ldots) + 9a_1 + 99a_2 \\ &\quad + 999a_{3+\ldots} \end{aligned}$$

and

$$9a_1 + 99a_2 + 999a_3 + \ldots \qquad (18)$$

is already divisible by 9.

Divisibility by 10

Any integer for which $a_0 = 0$ is itself divisible by 10 since

$$I = a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots \left| a_0 \right| \le 9$$
$$\text{and} \qquad 10a_1 + 100a_2 + 1000a_3 + \ldots \qquad (19)$$

is already divisible by 10.

Divisibility by 11

Any integer I for which $a_0 - a_1 + a_2 - a_3 + \ldots$ is divisible by 11 is itself divisible by 11 since

$$\begin{aligned} I &= a_0 + 10a_1 + 100a_2 + 1000a_3 + \ldots \\ &= a_0 + (11-1)a_1 + (99+1)a_2 + (1001-1)a_3 + \ldots \\ &= (a_0 - a_1 + a_2 - a_3 + \ldots) + 11a_1 + 99a_2 + 1001a_3 + \ldots \end{aligned}$$
$$\text{and} \qquad 11a_1 + 99a_2 + 1001a_3 + \ldots \qquad (20)$$

is already divisible by 11.

Remark: Following the pattern begun here, the rules for divisibility by any integer may similarly be developed.

The Divisor Function

divisor function $d(n)$**.** In number theory, a function that counts the number of divisors of a number n, including 1 and n. When p is prime, $d(p^a) = a + 1$. Since $d(n)$ is multiplicative (i.e., $d(n_1,n_2) = d(n_1)d(n_2)$), the value for any argument may be easily computed from its prime factorization; e.g., let $n = 12 = 2^2 \times 3$ so that $d(12) = d(2^2) \times d(3) = (2 + 1) \times (1 + 1) = 6$. The six divisors of 12 are 1, 2, 3, 4, 6, and 12.

The Sigma Function

sigma function $\sigma(n)$**.** In number theory, a function that sums the distinct divisors of a number n, including 1 and n. The sum of the proper factors of n (all the factors of n including 1 but excluding n) is therefore $\sigma(n) - n$. When p is prime, $\sigma(n) = (p^{(n+1)} - 1)/(p - 1)$. Since $\sigma(n)$ is multiplicative, the value for any argument may be computed from its prime factorization. (In terms of this function, a perfect number is one with $\sigma(n) = 2n$, and a pair of amicable numbers a and b have $\sigma(a) - a = b$ and $\sigma(b) - b = a$, or equivalently, $\sigma(a) = \sigma(b) = (a + b.)$; e.g., let $n = 12$. The factors of 12 are 1, 2, 3, 4, 6, and 12. The sum of these factors is 28. Now, $\sigma(12) = \sigma(2^2) \times \sigma(3) = \{(2^{(2+1)} - 1)/(2 - 1)\} \times \{(3^{(1+1)} - 1)/(3 - 1)\} = 7 \times 4 = 28$.

Appendix C

Implications and Equivalences

English Equivalents

$p \Rightarrow q$ is read

If $p(x_0)$ then $q(x_0)$
If $p(x_0)$, $q(x_0)$
$p(x_0)$ implies $q(x_0)$
$p(x_0)$ only if $q(x_0)$
$p(x_0)$ is a sufficient condition for $q(x_0)$
$p(x_0)$ is sufficient for $q(x_0)$
$p(x_0)$ only on the condition that $q(x_0)$
Whenever $p(x_0)$, $q(x_0)$
If $p(x_0)$, $q(x_0)$
Given that $p(x_0)$, $q(x_0)$
In case $p(x_0)$, $q(x_0)$
$q(x_0)$ is implied by $p(x_0)$
$q(x_0)$ if $p(x_0)$
$q(x_0)$ is a necessary condition for $p(x_0)$
$q(x_0)$ is necessary for $p(x_0)$
$q(x_0)$ on the condition that $p(x_0)$
$q(x_0)$ provided that $p(x_0)$

$p \Leftrightarrow q$ is read

$p(x_0)$ is equivalent to $q(x_0)$
$p(x_0)$ and $q(x_0)$ are equivalent
$p(x_0)$ implies and is implied by $q(x_0)$
$p(x_0)$ if and only if $q(x_0)$ [$p(x_0)$ iff $q(x_0)$]
$p(x_0)$ is a necessary and sufficient condition for $q(x_0)$
$p(x_0)$ is necessary and sufficient for $q(x_0)$
$p(x_0)$ just in case $q(x_0)$

Truth Values

$p \Rightarrow q$ is true if

[$p(x_0)$ is true and $q(x_0)$ is true] or
[$p(x_0)$ is false and $q(x_0)$ is true] or
[$p(x_0)$ is false and $q(x_0)$ is false]

$p \Rightarrow q$ is false (i.e., $\sim(p \Rightarrow q)$ is true) if

[$p(x_0)$ is true and $q(x_0)$ is false]

$p \Leftrightarrow q$ is true if

[$p(x_0)$ is true and $q(x_0)$ is true] or
[$p(x_0)$ is false and $q(x_0)$ is false]

$p \Leftrightarrow q$ is false (i.e., $\sim(p \Leftrightarrow q)$ is true) if

[$p(x_0)$ is true and $q(x_0)$ is false] or
[$p(x_0)$ is false and $q(x_0)$ is true]

Appendix D

Conjunctions and Disjunctions

English Equivalents

$p \wedge q$ is read

$p(x_0)$ and $q(x_0)$
$p(x_0)$, also $q(x_0)$
$p(x_0)$, but $q(x_0)$
$p(x_0)$, although $q(x_0)$
$p(x_0)$ as well as $q(x_0)$
Both $p(x_0)$ and $q(x_0)$
Though $p(x_0)$, $q(x_0)$

$p \vee q$ is read

$p(x_0)$ or $q(x_0)$
Either $p(x_0)$ or $q(x_0)$
$p(x_0)$ unless $q(x_0)$
[Also $\sim q \Rightarrow p$ is translated "p unless q"]

$\sim(p \vee q)$ is read

Neither $p(x_0)$ nor $q(x_0)$

Truth Values

$p \wedge q$ is true if

[$p(x_0)$ is true and $q(x_0)$ is true]

$p \wedge q$ is false if

[$p(x_0)$ is true and $q(x_0)$ is false] or
[$p(x_0)$ is false and $q(x_0)$ is true] or
[$p(x_0)$ is false and $q(x_0)$ is false]

$p \vee q$ is true if

[$p(x_0)$ is true and $q(x_0)$ is true] or
[$p(x_0)$ is true and $q(x_0)$ is false] or
[$p(x_0)$ is false and $q(x_0)$ is true]

$p \vee q$ is false if

[$p(x_0)$ is false and $q(x_0)$ is false]

Appendix E

Laws and Theorems of Logic

Law of Identity
$p \Leftrightarrow p$

Laws of Idempotence
$p \Leftrightarrow p \wedge p$
$p \Leftrightarrow p \vee p$

Law of Double Negation
$p \Leftrightarrow \sim\sim p$

Law of the Excluded Middle
$p \vee \sim p$ = true

Law of Contradiction
$p \wedge \sim p$ = false

Laws of Simplification
$p \wedge q \Rightarrow p$
$p \wedge q \Rightarrow q$

Law of Absurdity
$[p \Rightarrow (q \wedge \sim q)] \Rightarrow \sim p$
(also impossible antecedent)

Law of Addition
$p \Rightarrow p \vee q$

Law of the True Consequent
$q \Rightarrow (p \Rightarrow q)$

Law of the False Antecedent
$p \Rightarrow (\sim p \Rightarrow q)$ (also Law of Duns Scotus)

Law of Equivalence
$[(p \wedge q) \vee (\sim p \wedge \sim q)] \Leftrightarrow (p \Leftrightarrow q)$

Law of Negation
$\sim(p \Rightarrow q) \Leftrightarrow (p \wedge \sim q)$

Remark:
$(p \wedge \sim q) \Rightarrow (p \Leftrightarrow \sim q)$
$\sim(p \Leftrightarrow q) \Leftrightarrow [(p \wedge \sim q) \vee (\sim p \wedge q)]$

Remark:
$[(p \wedge \sim q) \vee (\sim p \wedge q)] \Leftrightarrow [(p \Leftrightarrow \sim q) \vee (\sim p \Leftrightarrow q)]$

Laws of Contraposition
$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
$(p \Leftrightarrow q) \Leftrightarrow (\sim q \Leftrightarrow \sim p)$

Law of Exportation
$[(p \wedge q) \Rightarrow r] \Rightarrow [p \Rightarrow (q \Rightarrow r)]$

Law of Importation
$[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \wedge q) \Rightarrow r]$

Law of Absorption
$(p \Rightarrow q) \Rightarrow [p \Rightarrow (p \wedge q)]$

Commutative Laws
$(p \vee q) \Leftrightarrow (q \vee p)$
$(p \wedge q) \Leftrightarrow (q \wedge p)$
$(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$

Associative Laws
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

Distributive Laws
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

De Morgan's Laws
$\sim(p \vee q) \Rightarrow \sim p \wedge \sim q$
$\sim(p \wedge q) \Rightarrow \sim p \vee \sim q$

Pierce's Law
$[(p \Rightarrow q) \Rightarrow p] \Rightarrow p$

Modus Ponendo Ponens
$(p \Rightarrow q) \wedge p \Rightarrow q$
(also affirming the antecedent or rule of detachment)

Modus Ponendo Tollens
$\sim(p \wedge q) \wedge p \Rightarrow \sim q$

Modus Tollendo Ponens
$(p \vee q) \wedge \sim p \Rightarrow q$
(also disjunctive syllogism)

Modus Tollendo Tollens
$(p \Rightarrow q) \wedge \sim q \Rightarrow \sim p$
(also denying the consequent)

Equivalence Ponens
$(p \Leftrightarrow q) \wedge p \Rightarrow q$ (or $(p \Leftrightarrow q) \wedge q \Rightarrow p$)

Equivalence Tollens
$(p \Leftrightarrow q) \wedge \sim p \Rightarrow$ ~q (or $(p \Leftrightarrow q) \wedge \sim q \Rightarrow \sim p$)

Hypothetical Syllogism
$(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$

Disjunctive Syllogism
$(p \vee q) \wedge \sim p \Rightarrow q$
(also modus tollendo ponens)

Simple Constructive Dilemma
$[(p \Rightarrow q) \wedge (r \Rightarrow q)] \wedge (p \vee r) \Rightarrow q$

Complex Constructive Dilemma
$[(p \Rightarrow q) \wedge (r \Rightarrow s)] \wedge (p \vee r) \Rightarrow q \vee s$

Simple Destructive Dilemma
$[(p \Rightarrow q) \wedge (p \Rightarrow r)] \wedge (\sim q \vee \sim r) \Rightarrow \sim p$

Complex Destructive Dilemma
$[(p \Rightarrow q) \wedge (r \Rightarrow s)] \wedge (\sim q \vee \sim s) \Rightarrow \sim p \vee \sim r$

Special Dilemma
$(p \Rightarrow q) \wedge (\sim p \Rightarrow q) \Rightarrow q$

Conjunction Introduction
$p,q \Rightarrow p \wedge q$

Disjunction Introduction
$p \Rightarrow (p \vee q)$

Appendix F

Laws and Theorems of Set Algebra

Idempotent
$A \cup A = A$
$A \cap A = A$

Associative
$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$
$A \Delta (B \Delta C) = (A \Delta B) \Delta C$

Commutative
$A \cup B = B \cup A$
$A \cap B = B \cap A$
$A \Delta B = B \Delta A$

Distributive
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$
$A \times (B \cup C) = (A \times B) \cup (A \times C)$
$A \times (B \cap C) = (A \times B) \cap (A \times C)$
$A \times (B \setminus C) = (A \times B) \setminus (\mathrm{A} \times C)$

Identity
$A \cup \Phi = A$
$A \cap U = A$
$A \cup U = U$
$A \cap \Phi = \Phi$
$A \Delta A = \Phi$
$A \Delta \Phi = A$

Adjunction
$A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$

Power sets
$2^A \cap 2^B = 2^{A \cap B}$
$2^A \cup 2^B \subset 2^{A \cup B}$

Complement
$(A^C)^C = A$
$U^C = \Phi$
$\Phi^C = U$
$A \subset B \Leftrightarrow B^C \subset A^C$
$A \cup A^C = U$
$A \cap A^C = \Phi$
$A \Delta A^C = U$
$A \Delta U = A^C$
$A \Delta B = (A \cup B) \cap (A^C \cup B^C)$

De Morgan's laws
$(A \cup B)^C = A^C \cap B^C$
$(A \cap B)^C = A^C \cup B^C$

Theorem: $S \subset T \Rightarrow S \cap T = S$
Theorem: $S \subset T \Rightarrow S \cup T = T$
Theorem: $S \subset T \Rightarrow T' \subset S'$
Theorem: $S \subset T \Rightarrow S \cup (T \setminus S) = T$

Appendix G

Properties of Continuous Functions

1. The *sum* of two continuous functions is continuous.

2. The *product* of two continuous functions is continuous.

3. The *quotient* of two continuous functions is continuous at any point or in any interval where the denominator is not zero.

4. If $f(x)$ is continuous at $x = a$ with $f(a) = \alpha$ and $g(y)$ is continuous at $y = \alpha$, then $h(x) = (g \times f)(x) = g[f(x)]$ is continuous at $x = a$.

5. The *constant* function $f(x) = c_0$ for all x and the *linear* function $f(x) = ax + b$ for all x are continuous at any point or in any interval. Also, any *polynomial* function is continuous, and any *rational* function is continuous at any point or in any interval where the denominator is not zero.

6. If f is continuous on a closed interval $[a,b]$ and if η is any real number between $f(a)$ and $f(b)$, then for some c in the open interval (a,b), $f(c) = \eta$ (called the Intermediate Value Theorem or Property).

7. If f is continuous on a closed interval $[a,b]$, then f is *bounded* on $[a,b]$. Furthermore, if S is the set of values $f(x)$ for x in $[a,b]$ and $M = \sup S$, then there is an ξ in $[a,b]$ such that $f(\xi) = M$ (and similarly for $m = \inf S$).

Appendix H

Definitions and Theorems From Calculus

Limits

Definition: The equation $\lim_{x\to a} f(x) = A$ means that for each neighborhood $N_pA = (A - p, A + p)$ there exists a punctured neighborhood $N_r^*a = (a - r,a) \cup (a,a + r)$ such that $f\left(N_r^*a\right) \subseteq N_pA$.

Definition: The equation $\lim_{x\uparrow a} f(x) = A$ (limit from the left or limit from below) means that for each neighborhood N_pA there exists a *left* neighborhood $L_ra = (a - r,a)$ such that $f(L_ra) \subseteq N_pA$.

Definition: The equation $\lim_{x\downarrow a} f(x) = A$ (limit from the right or limit from above) means that for each neighborhood N_pA there exists a *right* neighborhood $R_ra = (a,a + r)$ such that $f(R_ra) \subseteq N_pA$.

Definition: The function f is *continuous* at $x = a$ if $\lim_{x\to a} f(x) = f(a)$. Formally, f is continuous at a if to each $N_p f(a)$ there corresponds an N_ra such that $f(N_rA) \subseteq N_pf(a)$.

Theorem: $\lim_{x\to a} f(x) = A$ iff $\lim_{x\downarrow a} f(x) = \lim_{x\uparrow a} f(x) = A$.

Theorem: Suppose that for each number x in some punctured neighborhood of a point a, the number $g(x)$ is between $f(x)$ and $h(x)$ and suppose that $\lim_{x\to a} f(x) = A$ and $\lim_{x\to a} h(x) = A$. Then $\lim_{x\to a} g(x) = A$.

Theorem: If $\lim_{x\to a} f(x) = A$ and $\lim_{x\to a} g(x) = B$, then $\lim_{x\to a}[f(x) + g(x)] = A + B$.

Theorem: If the function g is continuous at the point L and if $\lim_{x\to a} f(x) = L$, then $\lim_{x\to a} g[f(x)] = g(L)$.

Theorem: The equations $\lim_{x\to a} f(x) = A$ and $\lim_{x\to a} [f(x) - A] = 0$ are equivalent.

Theorem: If $\lim_{x\to a} f(x) = A$ and $\lim_{x\to a} g(x) = B$, then $\lim_{x\to a} f(x) \times g(x) = AB$.

Theorem: If $\lim_{x\to a} f(x) = A$ and $\lim_{x\to a} g(x) = B \neq 0$, then $\lim_{x\to a} f(x)/\lim_{x\to a} g(x) = A/B$.

The Derivative

Definition: If x is a number in the domain of a function for which the following limit exists,

$$\lim_{h\to 0} \frac{\left\{f\left(x+h\right) - f\left(x\right)\right\}}{h} \qquad (21)$$

then the limit is called the "derivative" of $f(x)$ at x and is denoted $df(x)/dx$.

Definition: If $df(x)/dx$ exists at a particular point x, then $f(x)$ is said to be differentiable at that point.

Theorem: If f is differentiable at x, then f is continuous at x.

Theorem: If f is differentiable in an interval I and $df/dx \neq 0$ for each $x \in I$, then f^{-1} exists and is a differentiable function. Specifically,

$$\frac{d\left[f\left(x\right)\right]}{dx} = \frac{1}{\frac{\left[f^{-1}\left(y\right)\right]}{dy}} \qquad (22)$$

Theorem: Chain rule: If $f(x)$ and $g(x)$ are differentiable functions, then

$$\frac{df\left[g\left(x\right)\right]}{dx} = \frac{d\left\{f\left[g\left(x\right)\right]\right\}}{d\left[g\left(x\right)\right]} \frac{dg\left(x\right)}{dx} \qquad (23)$$

Theorem: If f and g are differentiable functions, then

$$\frac{d\left(f+g\right)}{dx} = \frac{df}{dx} + \frac{dg}{dx} \qquad (24a)$$

$$\frac{d(fg)}{dx} = f\left(\frac{dg}{dx}\right) + g\left(\frac{df}{dx}\right) \qquad (24b)$$

$$\frac{d\left(\frac{f}{g}\right)}{dx} = \frac{\left[g\left(\frac{df}{dx}\right) - f\left(\frac{dg}{dx}\right)\right]}{g}$$

provided that $g \neq 0$ (24c)

$$\frac{d(\alpha f + \beta g)}{dx} = \alpha\left(\frac{df}{dx}\right) + \beta\left(\frac{dg}{dx}\right) \qquad (24d)$$

where α and β are numbers.

Definition: If f and df/dx are differentiable functions, then the function d^2f/dx^2 is the derivative of df/dx and is called the "second derivative" of f.

Definition: A function is *continuous on an interval* if it is continuous at every point of the interval.

Theorem: If f is continuous on $[a,b]$, then there are numbers A and B such that $f([a,b]) = [A,B]$.

Theorem: Suppose that the greatest or least value of a function f in (a,b) is $f(m)$ where $m \in (a,b)$ and suppose that f is differentiable at m, then $(df/dx)|_m = 0$.

Rolle's theorem: If f is differentiable in (a,b) and continuous on $[a,b]$ and if $f(a) = f(b)$, then there exists at least one number $m \in (a,b)$ such that $(df/dx)|_m = 0$.

Theorem of the mean: If f is differentiable in (a,b) and continuous on [a,b] and if $b \neq a$, then there is a number $m \in (a,b)$ such that

$$\frac{\left[f(b) - f(a)\right]}{(b-a)} = \left(\frac{df}{dx}\right)\Big|_m \qquad (25)$$

Extended theorem of the mean: If f and g are differentiable in (a,b) and are continuous on $[a,b]$ and if $dg/dx \neq 0$ for $x \in (a,b)$, then there exists a point $m \in (a,b)$ such that

$$\frac{\left[f(b) - f(a)\right]}{\left[g(b) - g(a)\right]} = \left(\frac{\frac{df}{dx}}{\frac{dg}{dx}}\right)\Big|_m \qquad (26)$$

Theorem: Let f and g be differentiable in some interval I and suppose that at each $x \in I$, $df/dx = dg/dx$, then there exists a number C (independent of x) such that for each $x \in I$, $f(x) = g(x) + C$.

Theorem: Suppose that f is continuous on the interval I. If $df/dx > 0$ at every *interior* point x of I, then f is increasing in I. If $df/dx < 0$ at every interior point x of I, then f is decreasing in I.

Theorem: If $d^2f/dx^2 > 0$ at every interior point of an interval I, then the graph of f is concave up in I.
If $d^2f/dx2 < 0$ at every interior point of an interval I, then the graph of f is concave down in I.

The Partial Derivative

Definition: If the domain of a function is R^n, then f is called a "function on R^n."
If the range of a function on R^n is a subset of R^1, then the function is called a "scalar-valued function."
If the range of f is a subset of R^s where $s > 1$, then f is called a "vector-valued function."
$f(x,y,z) = (u,v)$ is a vector-valued function on R^3 with (vector) components u and v.

Definition: If r is a positive number, then the *neighborhood* $N_r a$ of radius r about the point $a \in R^n$ is the set

$$N_r a = \left\{x \,\middle|\, x \in R^n, |x - a| < r\right\} \qquad (27)$$

Since $|x - a|$ stands for the distance between the points x and a, $N_r a$ is the set of points of R^n that are less than r units from a; i.e., $N_r a$ is the interior of an n-dimensional sphere.

Definition: In R^n, the equation $\lim_{x \to a} f(x) = A$ means that for each neighborhood $N_p A$, there exists a punctured neighborhood $N_r^* a$ such that $f\left(N_r^* a\right) \subseteq N_p A$.

Definition: If $f(x,y)$ is a scalar-valued function on R^2, two (first-order) partial derivatives $\partial f(x,y)/\partial x$ and $\partial f(x,y)/\partial y$ may be defined by the equations

$$\frac{\partial f(x,y)}{\partial x} = \frac{\lim_{h\to 0}\left[f(x+h,y)-f(x,y)\right]}{h} \tag{28a}$$

$$\frac{\partial f(x,y)}{\partial y} = \frac{\lim_{h\to 0}\left[f(x,y+h)-f(x,y)\right]}{h} \tag{28b}$$

Definition: Second (and higher)-order derivatives may also be defined:

$$\frac{\partial^2 f(x,y)}{\partial x^2} \tag{29a}$$

$$\frac{\partial^2 f(x,y)}{\partial x \partial y} \tag{29b}$$

$$\frac{\partial^2 f(x,y)}{\partial y^2} \tag{29c}$$

$$\frac{\partial^2 f(x,y)}{\partial y \partial x} \tag{29d}$$

Theorem: If $\partial^2 f(x,y)/\partial x\partial y$ and $\partial^2 f(x,y)/\partial y\partial x$ are continuous at a point (x,y), then $\partial^2 f(x,y)/\partial x\partial y = \partial^2 f(x,y)/\partial y\partial x$

Theorem: Chain rule: Suppose that f is a scalar-valued function on R^2 whose domain is a vector-valued function $\mathbf{G}$ on R^1. Let $\mathbf{G}(x) = [g(x),h(x)] = \mathbf{G}(u,v)$ where $u = g(x)$ and $v = h(x)$. Define $w = w(x) = f(\mathbf{G}) = f(u,v)$. Then

$$\frac{dw}{dx} = \left(\frac{\partial w}{\partial u}\right)\frac{du}{dx} + \left(\frac{\partial w}{\partial v}\right)\frac{dv}{dx} \tag{30}$$

Theorem: Chain rule: Suppose that f is a scalar-valued function on R^2 whose domain is a vector-valued function $\mathbf{G}$ on R^2. Let $\mathbf{G}(x,y) = [g(x,y),h(x,y)] = \mathbf{G}(u,v)$ and define $w = w(x,y) = f(\mathbf{G}) = f(u,v)$. Then

$$\frac{\partial w}{\partial x} = \left(\frac{\partial w}{\partial u}\right)\frac{\partial u}{dx} + \left(\frac{\partial w}{\partial v}\right)\frac{\partial v}{\partial x} \tag{31}$$

and

$$\frac{\partial w}{\partial y} = \left(\frac{\partial w}{\partial u}\right)\frac{\partial u}{dy} + \left(\frac{\partial w}{\partial v}\right)\frac{\partial v}{\partial y} \tag{32}$$

The Integral

Definition: Let $[a,b]$ be a closed interval. A set of $n + 1$ points, $x_0, x_1, x_2,\ldots,x_n$ such that $a = x_0 < x_1 < x_2 < \ldots < x_n = b$, is called a "partition" of $[a,b]$. Let $\Delta x_i = x_i - x_{i-1}$ for each value of i. Then the value $u = \max(\Delta x_i)$ is called the "norm" of the partition.

Definition: Let $x_i^* \in [x_{i-1},x_i\ ]$. Then for some function $f(x)$, the sum $s = \sum_{i=1}^{n} f\left(x_i^*\right)\Delta x_i$ approximates the *area* under the graph of $f(x)$ over $[a,b]$.

Definition: Define by $S(u)$ the set of *all* the sums $s = \sum_{i=1}^{n} f\left(x_i^*\right)\Delta x_i$ for *all* partitions of a given norm u and *all* possible choices of x_i^* for each partition: $S(u) = \left\{ s \middle| s = \sum_{i=1}^{n} f\left(x_i^*\right)\Delta x_i \text{ for partition of norm } u \right\}$.

Note: Any subinterval $[x_{i-1},x_i]$ may be chosen as a norm of the partition, and the value x_j^* may be placed anywhere within the j^{th} subinterval. The equation

$$S(u) = \left\{ s \middle| s = \sum_{i=1}^{n} f\left(x_i^*\right)\Delta x_i \text{ for partition of norm } u \right\}$$

defines a set-valued function with domain $(0,b-a]$ (since $0 < u \le (b-a)$) and range, a family of sets $\{S(u)\}$. One thus has a rule that pairs with each of the numbers u in the domain one of the sets $S(u)$ in the range.

Definition: Let f be a function whose domain contains an interval $[a,b]$, and define a set-valued function $S(u)$ as above. Then, if $\lim_{u\downarrow 0} S(u)$ exists, f is said to

be *integrable* on [*a*,*b*]. The limit, called the "integral of *f* over [*a*,*b*]" is denoted $\int_a^b f(x)dx$.

Theorem: If *f* is integrable on [*a*,*b*] and if $f(x) > 0$ for each $x \in [a,b]$, then $\int_a^b f(x)dx \geq 0$.

Definition: For any function *f* whose domain consists of a (single) point *a*, $\int_a^a f(x)dx = 0$.

Definition: If $a < b$ and if *f* is integrable on [*a*,*b*], then $\int_a^b f(x)dx = -\int_b^a f(x)\,dx$.

Definition: The *measure* of a finite interval is its length.

The *measure* of a set containing a finite number of points is zero.

The union and intersection of two sets of measure zero have measure zero.

Every subset of a set of measure zero has measure zero.

Definition: A function *f* is bounded above on [*a*,*b*] if there exists a number *M* such that $M \geq f(x)$ for every $x \in [a,b]$. A function *f* is bounded below on [*a*,*b*] if there exists a number *M* such that $M \leq f(x)$ for every $x \in [a,b]$. A function *f* is bounded on [*a*,*b*] if it is bounded above and below.

Theorem: Existence of $\int_a^b f(x)dx$: A function *f* that is bounded on [*a*,*b*] is integrable on [*a*,*b*] if and only if the set of points in [*a*,*b*] at which *f* is discontinuous has measure zero. In particular, a bounded function is integrable on an interval if it has only a finite number of points of discontinuity. If *f* is unbounded on [*a*,*b*], then it is not integrable on [*a*,*b*].

Theorem: If *f* is integrable on [*a*,*b*] and *c* is a given number, then

$$\int_a^b cf(x)dx = c\int_a^b f(x)dx \qquad (33a)$$

$$\int_a^b \left[f(x) + g(x)\right]dx = \int_a^b f(x)dx + \int_a^b g(x)dx \qquad (33b)$$

Theorem: Mean value theorem for integrals: If *f* is continuous on [*a*,*b*], then there exists a number *m* $\in [a,b]$ such that $(b-a)f(m) = \int_a^b f(x)dx$.

Theorem: Let *a*, *b*, and *c* be three points of an interval that is contained in the domain of a function *f*. Then, if any two of the following integrals exists, so does the third, and

$$\int_a^c f(x)\,dx = \int_a^b f(x)dx + \int_b^c f(x)dx \qquad (34)$$

The Fundamental theorem of calculus: If a function *f* is integrable on [*a*,*b*] and if *F* is a function that is continuous on [*a*,*b*] such that $dF(x)/dx = f(x)$ for each $x \in [a,b]$, then

$$\int_a^b f(x)dx = F(b) - F(a) \qquad (35a)$$

also denoted

$$\int_a^b f(x)dx = F(x)\Big|_a^b \qquad (35b)$$

Definition: If *f* is integrable on an interval that contains a point *c*, then a function $F(x)$ may be defined as

$$F(x) = \int_c^x f(t)dt \qquad (36)$$

Theorem: If *f* is integrable on an interval *I* that contains a point *c*, then the function defined by $F(x) = \int_c^x f(t)dt$ is continuous on *I*.

Theorem: Suppose that *f* is integrable on an interval *I* that contains a point *c*, and *F* is the function defined by the equation $F(x) = \int_c^x f(t)dt$. Then if *f* is continuous at a point $x \in I$, *F* is differentiable at *x* and

$$\frac{dF(x)}{dx} = f(x) \tag{37}$$

or

$$\frac{d\left[\int_c^x f(t)dt\right]}{dx} = f(x) \tag{38}$$

provided that f is continuous at x.

The Multiple Integral

Definition: Let $f(x_1, x_2, \ldots x_n)$ be a function on R^n and let the domain of f contain an n-dimensional region

$$R = \{(x_1, x_2, \ldots x_n) | \alpha \le x_1 \le \beta, \gamma \le x_2 \le \delta, \ldots, \mu \le x_n \le \nu\} \tag{39}$$

where α, β,…, ν may be constants or functions of the coordinates. Call R the "region of integration." Partition R by dividing it into q differential subregions $\Delta V_i = \Delta x_{1i} \Delta x_{2i} \ldots \Delta x_{ni}$, $i \in \{1, 2, \ldots, q\}$ and define the norm of the partition to be the value $u = \max(\Delta V_i)$. Let the point $\left(x_{1i}^*, x_{2i}^*, \ldots, x_{ni}^*\right) \in \Delta V_i$. Form the sum

$$S = \sum_{i=1}^{q} f\left(x_{1i}^*, x_{2i}^*, \ldots, x_{ni}^*\right) \Delta V_i \tag{40}$$

Now, for *all* partitions of a given norm u and all possible choices of $\left(x_{1i}^*, x_{2i}^*, \ldots, x_{ni}^*\right)$ for each partition, define

$$S(u) = \left\{ s \middle| s = \sum_{i=1}^{q} f\left(x_{1i}^*, x_{2i}^*, \ldots, x_{ni}^*\right) \Delta V_i \text{ for a partition of norm } u \right\} \tag{41}$$

Then if $\lim_{u \downarrow 0} S(u)$ exists, f is said to be *integrable* on R. The limit, called the "integral of f over R" is denoted

$$\int_\alpha^\beta \int_\gamma^\delta \ldots \int_\mu^\nu f(x_1, x_2, \ldots x_n) dx_1 dx_2 \ldots dx_n \equiv \iint \ldots \int_R f dV \tag{42}$$

Some of the most important properties of single integrals are shared by multiple integrals; for example,

Theorem: If f and g are integrable on a region R and if m and n are any numbers, then

$$\iint \ldots \int_R (mf + ng) dV = m\left(\iint \ldots \int_R f dV\right) + n\left(\iint \ldots \int_R g dV\right) \tag{43}$$

Theorem: If f is integrable on a region R and if R may be divided into two non-overlapping subregions R_1 and R_2 such that $R = R_1 \cup R_2$ and $\Phi = R_1 \cap R_2$, then

$$\iint \ldots \int_R f dV = \iint \ldots \int_{R_1} f dV + \iint \ldots \int_{R_2} f dV \tag{44}$$

Appendix I

Real-Valued Functions as a Vector Space

Definition: A vector space V is a set of elements (called "vectors") defined over a field. The field elements are called "scalars." A vector space is closed with respect to a binary operation + between any two vectors and the binary operation $\bullet$ between any vector and any member of the field. In the following expansion, $\mathbf{x}$ and $\mathbf{y}$ represent vectors and α and β represent members of the field:

1. $\mathbf{x} + \mathbf{y}$ exists and is a unique member of V.
2. $\alpha \bullet \mathbf{x}$ exists and is a unique member of V.
3. Commutative laws: $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$ and $\alpha \bullet \mathbf{x} = \mathbf{x} \bullet \alpha$.
4. Distributive laws: $\alpha \bullet (\mathbf{x} + \mathbf{y}) = \alpha \bullet \mathbf{x} + \alpha \bullet \mathbf{y}$ and $(\alpha + \beta) \bullet \mathbf{x} = \alpha \bullet \mathbf{x} + \beta \bullet \mathbf{x}$.
5. Associative law: $(\alpha \bullet \beta) \bullet \mathbf{x} = \alpha \bullet (\beta \bullet \mathbf{x})$.
6. For $\alpha = 1$, $1 \bullet \mathbf{x} = \mathbf{x} \bullet 1 = \mathbf{x}$.

The set of all real-valued functions (here represented by $f(x)$ and $g(x)$) forms a vector space V over the field of real numbers (here represented by α and β) since for any two functions f and g with the same domain,

1. $f(x) + g(x)$ exists and is a member of V.
2. $\alpha \bullet f(x)$ exists and is a unique member of V.
3. Commutative laws: $f(x) + g(x) = g(x) + f(x)$ and $\alpha \bullet [f(x)] = [f(x)] \bullet \alpha$.
4. Distributive laws: $\alpha \bullet [f(x) + g(x)] = \alpha \bullet f(x) + \alpha \bullet g(x)$ and $(\alpha + \beta) \bullet f(x) = \alpha \bullet f(x) + \beta \bullet f(x)$.
5. Associative law: $(\alpha \bullet \beta) \bullet f(x) = \alpha \bullet [\beta \bullet f(x)]$.
6. For $\alpha = 1$, $\alpha \bullet [f(x)] = [f(x)] \bullet \alpha = f(x)$.

Appendix J

Logical Puzzles and Paradoxes

Epiminides paradox. Involves two philosophers who encounter a third along the way. The first philosopher states that everything the second says is true. The second asserts that the first is lying. Therefore, if the first is telling the truth, then he must be lying. But if he is lying, then he must be telling the truth.

Zeno's (Zeno of Elea, ca. 490 B.C.) ***paradoxes.*** A collection of paradoxes regarding time, motion, and plurality. The four best known are dichotomy, Achilles' paradox, the arrow paradox, and the stadium paradox.

*dichotomy paradox***.** That motion can never be initiated. Before a runner can traverse a distance, he must complete the first half of the distance, and before that, the first quarter, and so on, so that the runner cannot start until he has made the last in this infinite sequence of steps.

Achilles' paradox (also, the race course paradox)**.** That motion can never be completed. Achilles and a tortoise engage in a race in which the tortoise is given a head start. Before Achilles can overtake the tortoise, he must first reach its initial position. But by then, the tortoise has advanced farther along. The argument repeats indefinitely with the result that Achilles can never overtake the tortoise since to do so, he must cover an infinite number of distinct distances.

*arrow paradox***.** That motion is illusory. An object in flight always occupies a space equal to itself, but that which occupies a space equal to itself cannot be moving. Therefore the arrow must always be at rest.

*stadium paradox***.** That there can be no smallest unit (subdivision) of space or time. Two runners move from a given point in a stadium and proceed in opposite directions at a constant rate for one unit of time. In that one unit of time, they each move one unit of space, but relative to each other, they move two units of space. Therefore, relative to each other, they move one unit of space in one-half unit of time, and so there must always be a unit smaller than the supposed unit.

paradox of the heap. That there can be no such thing as a heap. One grain of sand is not a heap. If something is not a heap, then the addition of another single grain of sand will not make it a heap, i.e., by starting with a single grain, and adding to it one grain at a time, we will never make a heap. But then, nothing can be a heap, for if what we generate by the one-grain-at-a-time method is not a heap, then nothing like it arrived at by any other method can be a heap. Therefore, there are no heaps. Similarly, given a person who is not bald, plucking one hair from his/her head will not make the person bald. So, if we started plucking one hair at a time, we could never make a person bald. There can be no bald people.

Galileo's paradox. For infinite sets, the whole can be made equal to a part. Consider the unending sequence of positive integers 1, 2, 3, 4,… These integers may be put into a one-to-one correspondence with the sequence 2, 4, 6, 8,… by simply doubling each integer in the original sequence, or they may be put into a one-to-one correspondence with the sequence 1, 4, 9, 16,… by squaring each integer in the original sequence. But both derived sequences, 2, 4, 6, 8,… and 1, 4, 9, 16,… are apparently already contained in the original sequence 1, 2, 3, 4,…

dilemma of the crocodile. Involves a crocodile stealing a child and saying that he will return the child if the father can guess correctly whether or not he will do so. The father guesses that he will not. Therefore, if the crocodile does not return the child, the father is correct and he must return the child. But if the crocodile returns the child, then the father is not correct and the crocodile may keep the child.

paradox of identity. Based upon the statement, "If α is identical to β, then α and β have exactly the same properties (attributes)." From this statement, it is possible to conclude that no individual persists

through time. Any individual who is alive at a time t has a certain age n. At a later moment, say $t^* = t + \Delta t$, the individual will have another age, $n + \Delta t$. But, if age is a property (attribute) of an individual, then the individual who was alive at time t cannot be the same individual who was alive at time t^*. Thus, no individual can persist through time.

Paradox of the surprise 1-hour examination. That a surprise 1-hour examination will be given sometime next week is announced by the professor of a certain course at the end of class on Friday. A student reasons that the surprise exam cannot be given next Friday, since if it had not been given up until then, he would know after Thursday's class that the exam must be on Friday, and the element of surprise would be gone. Similarly, the exam cannot be given on Thursday because if it had not been given up until then, he would know after Wednesday's class that the exam must be on Thursday. And so on, working back to Monday. Therefore, since all the other days have now been eliminated, the surprise exam cannot be given on Monday without losing the element of surprise. Therefore, there can be no surprise exam.

prisoner's dilemma. A classic situation in which two prisoners are separated and each is told that if he confesses but the other does not, he will be released and receive a reward. If neither confesses, they will both have to be released without further penalty. If both confess, both will be convicted of a charge carrying an intermediate penalty. Each player has a dominant strategy (confess) which if used simultaneously, is worse for both than if one selects a nondominant (dominated) strategy (say nothing). The arms race may be viewed as a prisoner's dilemma. Two countries have nuclear armaments. Either may launch an attack and overpower the other (dominant strategy), but if both do so simultaneously, both will be destroyed. The dominated strategy is to *not* launch an attack but rather to maintain armed parity (i.e., a condition of mutually assured destruction).

Newcomb's problem. Involves a game show host with two boxes. Box A is transparent and is filled with $100 bills. Box B is opaque. The guest is told that box A contains $10,000 and that box B contains either $1 million or nothing. The guest is given the choice between taking only what is in box B or what is in both boxes. Before being allowed to choose, however, the guest is also told that on the basis of a detailed personality profile obtained before the show, the host has made a prediction about what choice will be made. The contents of box B are based upon this prediction. If the prediction was that the guest would take both boxes, then nothing was put into box B. If the prediction was that the guest would take only box B, then $1 million was put into it. The host claims to have made correct predictions 99.9 percent of the time he has played this game in the past. What should the guest do?

Goodman's paradox of induction. That induction from past experience provides identically strong evidence for incompatible predictions. Let *grue* be the quality of being green until a specified *future* time t_0, and then of being blue for all time afterward. Then everything that is or has been *green* is also *grue*. Past greenness provides grounds for predicting future greenness. But past gruenness provides grounds for predicting future blueness.

Hemple's paradox of induction. That logically equivalent statements are not equivalent for the purposes of confirmation by experience. Every sighting of a black raven confirms the hypothesis that all ravens are black or, equivalently, that all nonblack things are nonravens (law of contra-position). Both statements have the same universal affirmative form (i.e., all α are β). Therefore, each statement should be individually supported by observations that instantiate both its subject and its predicate. Also, because of their equivalence, whatever tends to confirm one statement must equally tend to confirm the other. Hence, observations of nonblack nonravens (such as white shirts) should tend to confirm the second statement and so also the first. But this situation is absurd. The paradox is resolved by using a restricted quantifier which says that ravens are all black, not that for all X if X is a raven then X is black.

Berry's paradox. A semantic paradox that results from classifying the positive integers in terms of the smallest number of English syllables needed to describe them. For example, 3, 628, 800 is describable in 5 syllables as "factorial 10." Now, there must be a least integer not describable in less that 19 syllables. However, the description, "The least integer not describable in less than 19 syllables," describes that same integer in only 18 syllables, thereby contradicting itself.

***Richard's paradox*.** Generated by supposing that it is possible to list all the real numbers between 0 and 1 that can be defined by a finite condition (i.e., one that may be described in a finite number of words). Now, it is possible by a diagonal process to define a number that differs from every number on any such list. However, the diagonal process is itself a finite condition. Therefore, any number so generated belongs in the list, and it is not possible ever to complete the list.

***Grelling's paradox*.** Deals with adjectives that describe themselves. For example, "short" describes itself, as does "polysyllabic." But "long" does not describe itself, and neither does "monosyllabic." The adjective "autological" means "self-describing." The adjective "heterological" means "not self-describing." Is the adjective "heterological" itself heterological or autological?

***barber paradox*.** Involves a barber in a village who shaves only those members of the village who do not shave themselves. Who shaves the barber? If the barber does, then he does not, but if he does not, then he does.

Russell's paradox in set theory**.** One that may be stated in terms of books which are catalogs of books. Type 1 catalogs (catalogs of classical literature or poetry) do not list themselves. Type 2 catalogs (catalogs of catalogs) do list themselves. It is desired to make up a catalog that lists the titles of all type 1 catalogs (and none of type 2). Should the new catalog include itself? If "yes," then it must be type 2 and therefore should not include itself. If "no," then it must be a type 1 and therefore cannot be complete unless it does include itself.

Appendix K

Basics of Aristotelian Logic

Definition by Genus and Species

A genus is a specific class that is divisible into other (sub)classes called species. Aristotle's definition of a given term by genus and species first specifies a characteristic belonging to the genus of the term being defined. A second characteristic, the "differentia," is then added to indicate the species. The characteristic supplied by the differentia distinguishes the term being defined from all other terms belonging to the same genus. For example, man is a rational animal. The genus is predicated of the species but not conversely: we do not say, "A rational animal is man." The species term contains more information than the genus term.

Propositions

A proposition is an assertion that proposes or denies something and is capable of being judged true or false. Three types of propositions used in logic are categorical, hypothetical, and disjunctive. The propositions of classical Aristotelian logic are categorical. A categorical proposition consists of a subject term and a predicate term connected by the copula "is." The predicate affirms or denies something about the subject. If *S* stands for subject and *P* for predicate, the general categorical schema is (some or all of) *S* is (or is not) *P*. A hypothetical proposition consists of an antecedent (hypothesis) and a consequent (conclusion) connected by the copula "If…then…" If these terms are represented, respectively, as *H* and *C*, the general hypothetical schema is "If *H*, then *C*." The disjunctive proposition consists of two disjuncts connected by the copula "Either…or…" If *P* and *Q* are the disjuncts, the general disjunctive schema is "either *P* or *Q*."

Categorical Propositions

categorical proposition. Any proposition consisting of a subject, a predicate, and a quantifier (e.g., "For all…," or "There exists…," or "All…," or "Some…").

subject. That about which the proposition speaks.

predicate. That which is said (predicated) of the subject (see table 2 for types of predicates).

term. The subject and/or the predicate in a categorical proposition.

TABLE 2.—EXAMPLES OF PREDICATION

Predicate type	Example
Genus	Animal
Differentia	Rational
Species	Man (rational animal)
Property	Ability to solve problems
Accident	Eye or hair color

inference. A form of argument from which conclusions are drawn from premises accepted as true.

immediate inference. A form of argument that comprises only a single categorical proposition; also, inferential argument without a middle (mediate) term (for comparison, see the entry "mediate inference").

moods of categorical propositions. The four moods of categorical propositions: universal affirmation (usually represented as *A*), universal negative (usually represented as *E*), particular affirmation (usually represented as *I*), and particular negative (usually represented as *O*). Table 3 gives examples of each.

TABLE 3.—MOODS[a] OF CATEGORICAL PROPOSITIONS

Preposition[b]	Mood
A: All *S* are *P*.	Universal affirmation
E: No *S* are *P*.	Universal negative
I: Some *S* are *P*.	Particular affirmation
O: Some *S* are not *P*.	Particular negative

[a]In some texts, "type" is the same as "mood."
[b]*A*, universal affirmation; *E*, universal negative; *I*, particular affirmation; *O*, particular negative.

square of opposition. A graphical construction showing the relationship between the four types or moods of immediate inference. These relationships may be stated as

1. If all *S* are *P*, then some *S* must be *P*. Thus, "Some *S* are *P*" is a lower alternative or subaltern to "All *S* are *P*."
2. If all *S* are *P*, then it is false that no *S* are *P*. Thus, "All *S* are *P*" and "No *S* are *P*" are contrary (literally, the opposite) statements.
3. If no *S* are *P*, then some *S* must be "not *P*." Thus, "Some *S* are not *P*" is a subaltern to "No *S* are *P*."
4. If all *S* are *P*, then it is false that some *S* are not *P*. Thus, "Some *S* are not *P*" is a contradiction (literally, speaking against) of "All *S* are *P*."
5. If no *S* are *P*, then it is false that some *S* are *P*. Thus, "Some *S* are *P*" is a contradiction of "No *S* are *P*."

These five relationships are shown graphically in figure 1.

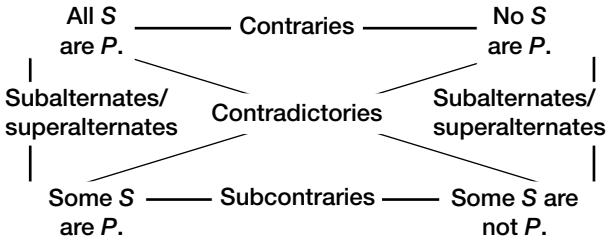

Figure 1.—Square of opposition.

truth value. The truth (T) or falsity (F) of a particular proposition.

truth table. A tabular construction showing all possible truth values for a proposition, given all possible truth values of its premise(s) and its conclusion(s); also, a tabular construction showing all possible truth values for certain propositions in an argument, given the truth value of other propositions in the argument. The example (table 4) shows the truth values of the categorical propositions (*A*, *E*, *I*, *O*) introduced above, given the truth value of one or two of them.

1. If *A* is true, then *E* must be false, *I* must be true, and *O* must be false.
2. If *A* is false, then *E* must be true, *I* must be false, and *O* must be true.
3. If *A* and *E* are both false, then *I* and *O* must both be true.

TABLE 4.—TRUTH TABLE FOR CATEGORICAL PROPOSITIONS

Proposition			
A	*E*	*I*	*O*
T	F	T	F
F	T	F	T
F	F	T	T

Table 5 shows the truth values of the same categorical propositions assuming the truth or falsity of each of *A*, *E*, *I*, and *O* sequentially:

converse. The converse of a categorical proposition is another categorical proposition in which the premise and conclusion are interchanged: "All *S* are *P*;" the converse is "All *P* are *S*."

TABLE 5.—INFERENCES DERIVED FROM ASSERTING THE TRUTH OR FALSITY OF A PARTICULAR CATEGORICAL PROPOSITION

Proposition	Inference		
If *A* is true	*E* is false	*I* is true	*O* is false
If *E* is true	*A* is false	*I* is false	*O* is true
If *I* is true	*A* is undetermined	*E* is false	*O* is undetermined
If *O* is true	*A* is false	*E* is undetermined	*I* is undetermined
If *A* is false	*E* is undetermined	*I* is undetermined	*O* is true
If *E* is false	*A* is undetermined	*I* is true	*O* is undetermined
If *I* is false	*A* is false	*E* is true	*O* is true
If *O* is false	*A* is true	*E* is false	*I* is true

TABLE 6.—CONVERSE, OBVERSE, CONTRAPOSITIVE, AND INVERSE OF CATEGORICAL PROPOSITIONS[a]

Proposition	Converse	Obverse	Contrapositive	Inverse[a]
All *S* are *P*.	All *P* are *S*.	No *S* are non-*P*.	All non-*P* are non-*S*.	All non-*S* are non-*P*.
No *S* are *P*.	No *P* are *S*.	All *S* are non-*P*.	All non-*P* are not non-*S*.	No non-*S* are non-*P*.
Some *S* are *P*.	Some *P* are *S*.	Some *S* are not non-*P*.	Some non-*P* are non-*S*.	Some non-*S* are non-*P*.
Some *S* are not *P*.	Some non-*P* are *S*.	Some *S* are not non-not *P*.	Some non-not *P* are non-*S*.	Some non-*S* are non-not *P*.

[a]*F*, full; *P*, partial.

obverse. The obverse of a categorical proposition is another categorical proposition that denies the opposite of the original proposition: "All *S* are *P*;" the opposite is "No *S* are *P*;" the obverse is "No *S* are not-*P*."

contrapositive. The contrapositive of a categorical proposition is another categorical proposition in which the premise and the conclusion are denied and interchanged: "All *S* are *P*;" the contrapositive is "All non-*P* are non-*S*."

inverse. The inverse of a categorical proposition is another categorical proposition in which the premise and the conclusion are denied: "All *S* are *P*;" the inverse is "All non-*S* are non-*P*." Table 6 presents these concepts.

Please note that such terms as "non-not *P*" are identical with *P*.

Categorical Syllogisms

syllogism. A form of mediate inference consisting of three categorical propositions: two premises (a major and a minor) and a conclusion. One term, the mediate (middle) term, must be common to both premises. The mediate term does not appear in the conclusion.

mediate inference. A form of argument that requires two or more premises; also, inference with a middle (mediate) term.

major premise. In a syllogism, the premise that contains the predicate of the conclusion.

minor premise. In a syllogism, the premise that contains the subject of the conclusion.

four figures of a syllogism. The particular distribution of subject, predicate, and middle term across the three premises of a syllogism; table 7 shows the four figures:

TABLE 7.—THE FOUR FIGURES[a]

First	Second	Third	Fourth
MP	*PM*	*MP*	*PM*
SM	*SM*	*MS*	*MS*
SP	*SP*	*SP*	*SP*

[a] *S*, subject term; *P*, predicate term; *M*, middle term.

distributed terms. Those terms in a proposition that refer to every member of the class being represented by the term. Table 8 shows the distribution of terms in the four moods of categorical propositions.

TABLE 8.—DISTRIBUTION OF TERMS[a] IN FOUR CATEGORICAL MOODS

Categorical mood	Distribution
A: All *S* are *P*.	The subject term is distributed; the predicate term is undistributed.
E: No *S* are *P*.	The subject and predicate terms are both distributed.
I: Some *S* are *P*.	The subject and predicate terms are both undistributed.
O: Some *S* are not *P*.	The subject term is undistributed; the predicate term is distributed.

[a]*S*, subject term; *P*, predicate term; *M*, middle term.

Figure 2 shows the same information in Venn diagram form:

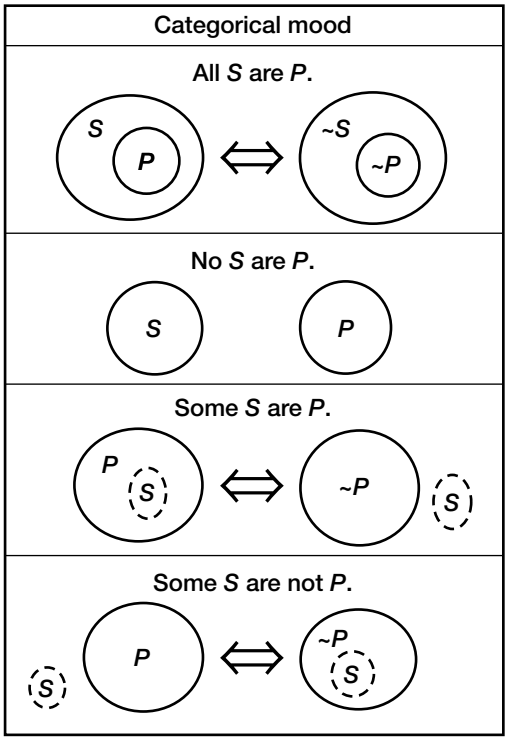

Figure 2.—Distribution of terms in four categorical moods, shown as class diagrams.

valid syllogisms. Each of the three categorical propositions in a syllogism must possess one of the four moods (*A*, *E*, *I*, and *O*). There are $4^3 = 64$ possible arrangements of these four moods over the three premises, but only 32 of these arrangements form valid syllogisms; the 32 arrangements are shown in table 9, arranged according to the four figures. For any given figure, there are only six valid arrangements of the four moods:

TABLE 9.—TWENTY-FOUR VALID SYLLOGISMS

Figure			
First	Second	Third	Fourth
AAA	*AEE*	*AAI*	*AAI*
AAI	*AEO*	*AII*	*AEE*
AII	*AOO*	*EAO*	*AEO*
EAE	*EAE*	*EIO*	*IAI*
EAO	*EAO*	*IAI*	*EAO*
EIO	*EIO*	*OAO*	*EIO*

Bibliography

1. Parker, Sybil P.: McGraw-Hill Dictionary of Mathematics. McGraw-Hill, New York, NY, 1997.
2. Daintith, J.; and Nelson, R.D.: The Penguin Dictionary of Mathematics. Penguin Books, 1989.
3. Clapham, Christopher: The Concise Oxford Dictionary of Mathematics. Second ed., Oxford University Press, Oxford, 1996.
4. Borowski, E.J.: The Harper Collins Dictionary of Mathematics. Harper Perennial, New York, NY, 1991.
5. Karush, William: Webster's New World Dictionary of Mathematics. Webster's New World, New York, NY, 1962.
6. Fisher, Robert Charles; and Ziebur, Allen D.: Calculus and Analytic Geometry. Prentice-Hall, Englewood Cliffs, NJ, 1965.
7. Perry, John; and Bratman, Michael S.: Introduction to Philosophy: Classical and Contemporary Readings. Oxford University Press, Oxford, 1986.
8. Milewski, Emig G.: The Topology Problem Solver: A Complete Solution Guide to Any Textbook. Research and Education Association, Piscataway, NJ, 1994.
9. Lipschutz, Seymour: Schaum's Outline of Theory and Problems of General Topology. Schaum Publishing Company, New York, NY, 1965.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 2003	Technical Paper

4. TITLE AND SUBTITLE

Concepts of Mathematics for Students of Physics and Engineering: A Dictionary

5. FUNDING NUMBERS

WBS–22–755–60–04–00

6. AUTHOR(S)

Joseph C. Kolecki

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135–3191

8. PERFORMING ORGANIZATION REPORT NUMBER

E–13741

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546–0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA TP—2003-212088

11. SUPPLEMENTARY NOTES

Responsible person, Joseph C. Kolecki, organization code 5410, 216–433–2296.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Categories: 31, 59, and 70 Distribution: Standard

Available electronically at http://gltrs.grc.nasa.gov

This publication is available from the NASA Center for AeroSpace Information, 301–621–0390.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 words)***

A physicist with an engineering background, the author presents a mathematical dictionary containing material encountered over many years of study and professional work at NASA. This work is a compilation of the author's experience and progress in the field of study represented and consists of personal notes and observations that can be used by students in physics and engineering.

14. SUBJECT TERMS

Dictionary; Physics; Mathematics; Engineering

15. NUMBER OF PAGES

51

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	