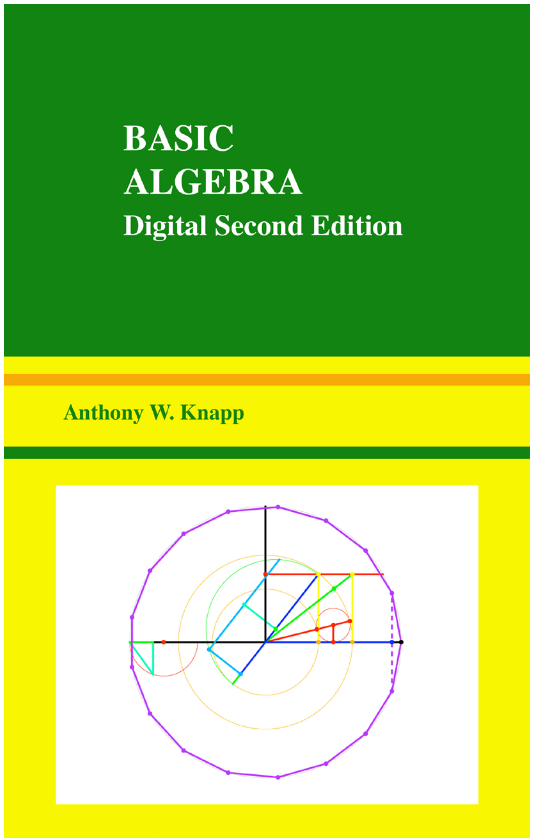
BASIC
ALGEBRA
Digital Second Edition
Anthony W. Knapp

Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/∼aknapp

Title: Basic Algebra
Cover: Construction of a regular heptadecagon, the steps shown in color sequence; see page 505.

Mathematics Subject Classification (2010): 15–01, 20–01, 13–01, 12–01, 16–01, 08–01, 18A05, 68P30.

First Edition, ISBN-13 978-0-8176-3248-9
c 2006 Anthony W. Knapp
Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN
c 2016 Anthony W. Knapp
Published by the Author

APPENDIX

Abstract. This appendix treats some topics that are likely to be well known by some readers and less known by others. Most of it already comes into play by Chapter II. Section A1 deals with set theory and with functions: it discusses the role of formal set theory, it works in a simplified framework that avoids too much formalism and the standard pitfalls, it establishes notation, and it mentions some formulas. Some emphasis is put on distinguishing the image and the range of a function, since this distinction is important in algebra and algebraic topology.

Section A2 defines equivalence relations and establishes the basic fact that they lead to a partitioning of the underlying set into equivalence classes.

Section A3 reviews the construction of rational numbers from the integers, and real numbers from the rational numbers. From there it concentrates on the solvability within the real numbers of certain polynomial equations.

Section A4 is a quick review of complex numbers, real and imaginary parts, complex conjugation, and absolute value.

Sections A5 and A6 return to set theory. Section A5 defines partial orderings and includes Zorn's Lemma, which is a powerful version of the Axiom of Choice, while Section A6 concerns cardinality.

A1. Sets and Functions

Algebra typically makes use of an informal notion of set theory and notation for it in which sets are described by properties of their elements and by operations on sets. This informal set theory, if allowed to be too informal, runs into certain paradoxes, such as **Russell's paradox:** "If S is the set of all sets that do not contain themselves as elements, is S a member of S or is it not?" The conclusion of Russell's paradox is that the "set" of all sets that do not contain themselves as elements is not in fact a set.

Mathematicians' experience is that such pitfalls can be avoided completely by working within some formal axiom system for sets, of which there are several that are well established. A basic one is "Zermelo–Fraenkel set theory," and the remarks in this section refer specifically to it but refer to the others at least to some extent.[1]

The standard logical paradoxes are avoided by having sets, elements (or "entities"), and a membership relation $\in$ such that $a \in S$ is a meaningful statement,

[1] Mathematicians have no proof that this technique avoids problems completely. Such a proof would be a proof of the consistency of a version of mathematics in which one can construct the integers, and it is known that this much of mathematics cannot be proved to be consistent unless it is in fact inconsistent.

true or false, if and only if a is an element and S is a set. The terms **set**, **element**, and $\in$ are taken to be primitive terms of the theory that are in effect defined by a system of axioms. The axioms ensure the existence of many sets, including infinite sets, and operations on sets that lead to other sets. To make full use of this axiom system, one has to regard it as occurring in the framework of certain rules of logic that tell the forms of basic statements (namely, $a = b$, $a \in S$, and "S is a set"), the connectives for creating complicated statements from simple ones ("or," "and," "not," and "if . . . then"), and the way that quantifiers work ("there exists" and "for all").

Working rigorously with such a system would likely make the development of mathematics unwieldy, and it might well obscure important patterns and directions. In practice, therefore, one compromises between using a formal axiom system and working totally informally; let us say that one works "informally but carefully." The logical problems are avoided not by rigid use of an axiom system, but by taking care that sets do not become too "large": one limits the sets that one uses to those obtained from other sets by set-theoretic operations and by passage to subsets.[2]

A feature of the axiom system lying behind working informally but carefully is that it does not preclude the existence of additional sets beyond those forced to exist by the axioms. Thus, for example, in the subject of coin-tossing within probability, it is normal to work with the set of possible outcomes as $S = \{\text{heads, tails}\}$ even though it is not immediately apparent that requiring this S to be a set does not introduce some contradiction.

It is worth emphasizing that the points of the theory at which one takes particular care vary somewhat from subject to subject within mathematics. For example it is sometimes of interest in calculus of several variables to distinguish between the range of a function and its image in a way that will be mentioned below, but it is usually not too important. In homological algebra, however, the distinction is extremely important, and the subject loses a great deal of its impact if one blurs the notions of range and image.

Some references for set theory that are appropriate for reading *once* are Halmos's *Naive Set Theory*, Hayden–Kennison's *Zermelo–Fraenkel Set Theory*, and Chapter 0 and the appendix of Kelley's *General Topology*. The Kelley book is one that uses the word "class" as a primitive term more general than "set"; it develops von Neumann set theory.

All that being said, let us now introduce the familiar terms, constructions, and notation that one associates with set theory. To cut down on repetition, one

[2] Not every set so obtained is to be regarded as "constructed." The Axiom of Choice, which we come to shortly, is an existence statement for elements in products of sets, and the result of applying the axiom is a set that can hardly be viewed as "constructed."

allows some alternative words for "set," such as **family** and **collection**. The word "class" is used by some authors as a synonym for "set," but the word **class** is used in some set-theory axiom systems to refer to a more general notion than "set," and it will be useful to preserve this possibility. Thus a class can be a set, but we allow ourselves to speak, for example, of the class of all groups even though this class is too large to be a set. Alternative terms for "element" are **member** and **point**; we shall not use the term "entity." Instead of writing $\in$ systematically, we allow ourselves to write "in." Generally, we do not use $\in$ in sentences of text as an abbreviation for an expression like "is in" that contains a verb.

If A and B are two sets, some familiar operations on them are the **union** $A \cup B$, the **intersection** $A \cap B$, and the **difference** $A - B$, all defined in the usual way in terms of the elements they contain. Notation for the difference of sets varies from author to author; some other authors write $A \setminus B$ or $A \sim B$ for difference, but this book uses $A - B$. If one is thinking of A as a universe, one may abbreviate $A - B$ as B^c, the **complement** of B in A. The empty set $\varnothing$ is a set, and so is the set of all subsets of a set A, which is sometimes denoted by 2^A. Inclusion of a subset A in a set B is written $A \subseteq B$ or $B \supseteq A$; then B is a superset of A. Inclusion that does not permit equality is denoted by $A \subsetneqq B$ or $B \supsetneqq A$; in this case one says that A is a **proper subset** of B or that A is **properly contained** in B.

If A is a set, the **singleton** $\{A\}$ is a set with just the one member A. Another operation is **unordered pair**, whose formal definition is $\{A, B\} = \{A\} \cup \{B\}$ and whose informal meaning is a set of two elements in which we cannot distinguish either element over the other. Still another operation is **ordered pair**, whose formal definition is $(A, B) = \{\{A\}, \{A, B\}\}$. It is customary to think of an ordered pair as a set with two elements in which one of the elements can be distinguished as coming first.[3]

Let A and B be two sets. The set of all ordered pairs of an element of A and an element of B is a set denoted by $A \times B$; it is called the **product** of A and B or the **Cartesian product**. A **relation** between a set A and a set B is a subset of $A \times B$. Functions, which are to be defined in a moment, provide examples. Two examples of relations that are usually not functions are "equivalence relations," which are discussed in Section A2, and "partial orderings," which are discussed in Section A5.

If A and B are sets, a relation f between A and B is said to be a **function**, written $f : A \to B$, if for each $x \in A$, there is exactly one $y \in B$ such that (x, y) is in f. If (x, y) is in f, we write $f(x) = y$. In this informal but careful definition of function, the function consists of more than just a set of ordered

[3] Unfortunately a "sequence" gets denoted by $\{x_1, x_2, \dots\}$ or $\{x_n\}_{n=1}^{\infty}$. If its notation were really consistent with the above definitions, we might infer, inaccurately, that the order of the terms of the sequence does not matter. The notation for unordered pairs, ordered pairs, and sequences is, however, traditional, and it will not be changed here.

pairs; it consists of the set of ordered pairs regarded as a subset of $A \times B$. This careful definition makes it meaningful to say that the set A is the **domain**, the set B is the **range**,[4] and the subset of $y \in B$ such that $y = f(x)$ for some $x \in A$ is the **image** of f. The image is also denoted by $f(A)$. Sometimes a function f is described in terms of what happens to typical elements, and then the notation is $x \mapsto f(x)$ or $x \mapsto y$, possibly with y given by some formula or by some description in words about how it is obtained from x. Sometimes a function f is written as $f(\,\cdot\,)$, with a dot indicating the placement of the variable; this notation is especially helpful in working with restrictions, which we come to in a moment, and with functions of two variables when one of the variables is held fixed. This notation is useful also for functions that involve unusual symbols, such as the absolute value function $x \mapsto |x|$, which in this notation becomes $|\cdot|$. The word **map** or **mapping** is used for "function" and for the operation of a function, especially when a geometric setting for the function is of importance.

Often mathematicians are not so careful with the definition of function. Depending on the degree of informality that is allowed, one may occasionally refer to a function as $f(x)$ when it should be called f or $x \mapsto f(x)$. If any confusion is possible, it is wise to use the more rigorous notation. Another habit of informality is to regard a function $f : A \to B$ as simply a set of ordered pairs. Thus two functions $f_1 : A \to B$ and $f_2 : A \to C$ become the same if $f_1(a) = f_2(a)$ for all a in A. With the less-careful definition, the notion of the range of a function is not really well defined. The less-careful definition can lead to trouble in algebra and topology, but it does not often lead to trouble in analysis until one gets to a level where algebra and analysis merge somewhat. One place where it comes into play in algebra is in the notion of an exact sequence of three abelian groups $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$, which is defined as a system of three abelian groups and homomorphisms as indicated such that the kernel of ψ equals the image of φ. In this definition one is not free to adjust B to be the image of φ since that adjustment will affect the kernel of ψ as well.

The set of all functions from a set A to a set B is a set. It is sometimes denoted by B^A. The special case 2^A that arises with subsets comes by regarding 2 as a set $\{1, 2\}$ and identifying a function f from A into $\{1, 2\}$ with the subset of all elements x of A for which $f(x) = 1$.

If a subset B of a set A may be described by some distinguishing property P of its elements, we may write this relationship as $B = \{x \in A \mid P\}$. For example the function f in the previous paragraph is identified with the subset $\{x \in A \mid f(x) = 1\}$. Another example is the image of a general function $f : A \to B$, namely $f(A) = \{y \in B \mid y = f(x) \text{ for some } x \in A\}$. Still more generally along these lines, if E is any subset of A, then $f(E)$ denotes the set

[4] Some authors refer to B as the **codomain**.

$\{y \in B \mid y = f(x) \text{ for some } x \in E\}$. Some authors use a colon or semicolon or comma instead of a vertical line in this notation.

This book frequently uses sets denoted by expressions like $\bigcup_{x \in S} A_x$, an indexed union, where S is a set that is usually nonempty. If S is the set $\{1, 2\}$, this reduces to $A_1 \cup A_2$. In the general case it is understood that we have an unnamed function, say f, given by $x \mapsto A_x$, having domain S and range the set of all subsets of an unnamed set T, and $\bigcup_{x \in S} A_x$ is the set of all $y \in T$ such that y is in A_x for some $x \in S$. When S is understood, we may write $\bigcup_x A_x$ instead of $\bigcup_{x \in S} A_x$. Indexed intersections $\bigcap_{x \in S} A_x$ are defined similarly, and this time it is essential to disallow S empty because otherwise the intersection cannot be a set in any useful set theory.

There is also an indexed **Cartesian product** $\bigtimes_{x \in S} A_x$ that specializes in the case that $S = \{1, 2\}$ to $A_1 \times A_2$. Usually S is assumed nonempty. This Cartesian product is the set of all functions f from S into $\bigcup_{x \in S} A_x$ such that $f(x)$ is in A_x for all $x \in S$. In the special case that S is $\{1, \dots, n\}$, the Cartesian product is the set of ordered n-tuples from n sets $A_1, \dots, A_n$ and may be denoted by $A_1 \times \cdots \times A_n$; its members may be denoted by $(a_1, \dots, a_n)$ with $a_j \in A_j$ for $1 \leq j \leq n$. When the factors of a Cartesian product have some additional algebraic structure, the notation for the Cartesian product is often altered; for example the Cartesian product of groups A_x is denoted by $\prod_{x \in S} A_x$.

It is completely normal in algebra, and it is the practice in this book, to take the following axiom as part of one's set theory; the axiom is customarily used without specific mention.

Axiom of Choice. The Cartesian product of nonempty sets is nonempty.

If the index set is finite, then the Axiom of Choice reduces to a theorem of set theory. The axiom is often used quite innocently with a countably infinite index set. For example a theorem of analysis asserts that any bounded sequence $\{a_n\}$ of real numbers has a subsequence converging to $\limsup a_n$, and the proof constructs one member of the sequence at a time. When the proof is written in such a way that these members have some flexibility in their definitions, the Axiom of Choice is usually being invoked. The proof can be rewritten so that the members of the subsequence have specific definitions, such as "the term a_n such that n is the smallest integer satisfying such-and-such properties." In this case the axiom is not being invoked. In fact, one can often rewrite proofs involving a countably infinite choice so that they involve specific definitions and therefore avoid invoking the axiom, but there is no point in undertaking this rewriting. In algebra the axiom is often invoked in situations in which the index set is uncountable; selection of a representative from each of uncountably many equivalence classes is such a choice if all equivalence classes have more than one element.

From the Axiom of Choice, one can deduce a powerful tool known as Zorn's Lemma, whose use it is customary to acknowledge. Zorn's Lemma appears in Section A5.

If $f : A \to B$ is a function and B is a subset of B', then f can be regarded as a function with range B' in a natural way. Namely, the set of ordered pairs is unchanged but is to be regarded as a subset of $A \times B'$ rather than $A \times B$.

Let $f : A \to B$ and $g : B \to C$ be two functions such that the range of f equals the domain of g. The **composition** $g \circ f : A \to C$, written sometimes as $gf : A \to C$, is the function with $(g \circ f)(x) = g(f(x))$ for all x. Because of the construction in the previous paragraph, it is meaningful to define the composition more generally when the range of f is merely a subset of the domain of g.

A function $f : A \to B$ is said to be **one-one** if $f(x_1) \neq f(x_2)$ whenever x_1 and x_2 are distinct members of A. The function is said to be **onto**, or often "onto B," if its image equals its range. The terminology "onto B" avoids confusion: it specifies the image and thereby guards against the use of the less careful definition of function mentioned above. A mathematical audience often contains some people who use the more careful definition of function and some people who use the less careful definition. For the latter kind of person, a function is always onto something, namely its image, and a statement that a particular function is onto might be regarded as a tautology. A function from one set to another is said to put the sets in **one-one correspondence** if the function is one-one and onto.

When a function $f : A \to B$ is one-one and is onto B, there exists a function $g : B \to A$ such that $g \circ f$ is the identity function on A and $f \circ g$ is the identity function on B. The function g is unique, and it is defined by the condition, for $y \in B$, that $g(y)$ is the unique $x \in A$ with $f(x) = y$. The function g is called the **inverse function** of f and is often denoted by f^{-1}.

Conversely if $f : A \to B$ has an inverse function, then f is one-one and is onto B. The reason is that a composition $g \circ f$ can be one-one only if f is one-one, and in addition, that a composition $f \circ g$ can be onto the range of f only if f is onto its range.

If $f : A \to B$ is a function and E is a subset of A, the **restriction** of f to E, denoted by $f\big|_E$, is the function $f : E \to B$ consisting of all ordered pairs $(x, f(x))$ with $x \in E$, this set being regarded as a subset of $E \times B$, not of $A \times B$. One especially common example of a restriction is restriction to one of the variables of a function of two variables, and then the idea of using a dot in place of a variable can be helpful notationally. Thus the function of two variables might be indicated by f or $(x, y) \mapsto f(x, y)$, and the restriction to the first variable, for fixed value of the second variable, would be $f(\,\cdot\,, y)$ or $x \mapsto f(x, y)$.

We conclude this section with a discussion of direct and inverse images of sets under functions. If $f : A \to B$ is a function and E is a subset of A, we have defined $f(E) = \{y \in B \mid y = f(x) \text{ for some } x \in E\}$. This is the same as the image of $f\big|_E$ and is frequently called the image or **direct image** of E under f. The notion of direct image does not behave well with respect to some set-theoretic operations: it respects unions but not intersections. In the case of unions, we have

$$f\Big(\bigcup_{s\in S} E_s\Big) = \bigcup_{s\in S} f(E_s);$$

the inclusion $\supseteq$ follows since $f\Big(\bigcup_{s\in S} E_s\Big) \supseteq f(E_s)$ for each s, and the inclusion $\subseteq$ follows because any member of the left side is f of a member of some E_s. In the case of intersections, the question $f(E\cap F) \overset{?}{=} f(E)\cap f(F)$ can easily have a negative answer, the correct general statement being $f(E\cap F) \subseteq f(E)\cap f(F)$. An example with equality failing occurs when $A = \{1,2,3\}$, $B = \{1,2\}$, $f(1) = f(3) = 1$, $f(2) = 2$, $E = \{1,2\}$ and $F = \{2,3\}$ because $f(E\cap F) = \{2\}$ and $f(E)\cap f(F) = \{1,2\}$.

If $f : A \to B$ is a function and E is a subset of B, the **inverse image** of E under f is the set $f^{-1}(E) = \{x \in A \mid f(x) \in E\}$. This is well defined even if f does not have an inverse function. (If f does have an inverse function f^{-1}, then the inverse image of E under f coincides with the direct image of E under f^{-1}.)

Unlike direct images, inverse images behave well under set-theoretic operations. If $f : A \to B$ is a function and $\{E_s \mid s \in S\}$ is a set of subsets of B, then

$$\begin{aligned} f^{-1}\Big(\bigcap_{s\in S} E_s\Big) &= \bigcap_{s\in S} f^{-1}(E_s),\\ f^{-1}\Big(\bigcup_{s\in S} E_s\Big) &= \bigcup_{s\in S} f^{-1}(E_s),\\ f^{-1}(E_s^c) &= (f^{-1}(E_s))^c. \end{aligned}$$

In the third of these identities, the complement on the left side is taken within B, and the complement on the right side is taken within A. To prove the first identity, we observe that $f^{-1}\big(\bigcap_{s\in S} E_s\big) \subseteq f^{-1}(E_s)$ for each $s \in S$ and hence $f^{-1}\big(\bigcap_{s\in S} E_s\big) \subseteq \bigcap_{s\in S} f^{-1}(E_s)$. For the reverse inclusion, if x is in $\bigcap_{s\in S} f^{-1}(E_s)$, then x is in $f^{-1}(E_s)$ for each s and thus $f(x)$ is in E_s for each s. Hence $f(x)$ is in $\bigcap_{s\in S} E_s$, and x is in $f^{-1}\big(\bigcap_{s\in S} E_s\big)$. This proves the reverse inclusion. The second and third identities are proved similarly.

A2. Equivalence Relations

An **equivalence relation** on a set S is a relation between S and itself, i.e., is a subset of $S \times S$, satisfying three defining properties. We use notation like $a \simeq b$, written "a is equivalent to b," to mean that the ordered pair (a, b) is a member of the relation, and we say that "$\simeq$" is the equivalence relation. The three defining properties are

(i) $a \simeq a$ for all a in S, i.e., $\simeq$ is **reflexive**,
(ii) $a \simeq b$ implies $b \simeq a$ if a and b are in S, i.e., $\simeq$ is **symmetric**.
(iii) $a \simeq b$ and $b \simeq c$ together imply $a \simeq c$ if a, b, and c are in S, i.e., $\simeq$ is **transitive**.

An example occurs with S equal to the set $\mathbb{Z}$ of integers with $a \simeq b$ meaning that the difference $a - b$ is even. The properties hold because (i) 0 is even, (ii) the negative of an even integer is even, and (iii) the sum of two even integers is even.

There is one fundamental result about abstract equivalence relations. The **equivalence class** of a, written $[a]$ for now, is the set of all members b of S such that $a \simeq b$.

Proposition. If $\simeq$ is an equivalence relation on a set S, then any two equivalence classes are disjoint or equal, and S is the union of all the equivalence classes.

PROOF. Let $[a]$ and $[b]$ be the equivalence classes of members a and b of S. If $[a] \cap [b] \neq \varnothing$, choose c in the intersection. Then $a \simeq c$ and $b \simeq c$. By (ii), $c \simeq b$, and then by (iii), $a \simeq b$. If d is any member of $[b]$, then $b \simeq d$. From (iii), $a \simeq b$ and $b \simeq d$ together imply $a \simeq d$. Thus $[b] \subseteq [a]$. Reversing the roles of a and b, we see that $[a] \subseteq [b]$ also, whence $[a] = [b]$. This proves the first conclusion. The second conclusion follows from (i), which ensures that a is in $[a]$, hence that every member of S lies in some equivalence class. □

EXAMPLE. With the equivalence relation on $\mathbb{Z}$ that $a \simeq b$ if $a - b$ is even, there are two equivalence classes—the subset of even integers and the subset of odd integers.

The first two examples of equivalence relations in this book arise in Section II.3. The first example, which is captured in the definition of square matrices that are "similar," yields equivalence classes exactly as above. A square matrix A is similar to a square matrix B if there is a matrix C with $B = C^{-1}AC$. The text does not mention in Chapter II that similarity is an equivalence relation, but it is routine to check that it is reflexive, symmetric, and transitive. The second example is a relation "is isomorphic to" and implicitly is defined on the class of all vector spaces. This class is not a set, and Section A1 of this appendix suggested avoiding using classes that are not sets in order to avoid the logical paradoxes mentioned at the beginning of the appendix. There is not much problem with using general classes in this particular situation, but there is a simple approach in this situation for eliminating classes that are not sets and thereby following the suggestion of Section A1 without making an exception. The approach is to work with any subclass of vector spaces that is a set. The equivalence relation is well defined on the set of vector spaces in question, and the proposition yields equivalence classes within that set. This set can be an arbitrary subclass of the class of all vector spaces that happens to be a set, and the practical effect is the same as if the equivalence relation had been defined on the class of all vector spaces.

A3. Real Numbers

Real numbers are taken as known, as are the rational numbers from which they are constructed. It will be useful, however, to review the constructions of both these number systems so as to be able to discuss the solvability of polynomial equations better.

We take the set $\mathbb{Z}$ of integers as given, along with its ordering and its operations of addition, subtraction, and multiplication. The set $\mathbb{Q}$ of rational numbers is constructed rigorously from $\mathbb{Z}$ as follows. We start from the set of ordered pairs (a, b) of integers such that $b \neq 0$. The idea is that (a, b) is to correspond to a/b and that we want (na, nb) to correspond to the same a/b if n is any nonzero integer. Thus we say that two such pairs have $(a, b) \sim (c, d)$ if $ad = bc$. This relation is evidently reflexive and symmetric, and it will be an equivalence relation if it is transitive. If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$. So $adf = bcf = bde$. Since $d \neq 0$, $af = be$ and $\sim$ is transitive.

From Section A2 the set of such pairs is partitioned into equivalence classes by means of $\sim$. Each equivalence class is called a **rational number**. To define the arithmetic operations on rational numbers, we first define operations on pairs, and then we check that the operations respect the partitioning into classes. For addition, the definition is $(a, b) + (c, d) = (ad + bc, bd)$. What needs checking is that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $(ad + bc, bd) \sim (a'd' + b'c', b'd')$. This is a routine matter: $(ad + bc)(b'd') = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')bd$, and thus addition of rational numbers is well defined. The operations on pairs for negative, multiplication, and reciprocal are $-(a, b) = (-a, b)$, $(a, b)(c, d) = (ac, bd)$, and $(a, b)^{-1} = (b, a)$, and we readily check that these define corresponding operations on rational numbers. Finally one derives the familiar associative, commutative, and distributive laws for these operations on $\mathbb{Q}$.

The above construction is repeated, with more details, in the more general construction of "fields of fractions" in Chapter VIII.

Inequalities on rational numbers are defined from inequalities on integers, taking into account that an inequality between integers is preserved when multiplied by a positive integer. Each rational number has a representative pair (a, b) with $b > 0$ because any pair can always be replaced by the pair of negatives. Thus let (a, b) and (c, d) be given with $b > 0$ and $d > 0$. We say that $(a, b) \leq (c, d)$ if $ad \leq bc$. One readily checks that this ordering respects equivalence classes and leads to the usual properties of the ordering on $\mathbb{Q}$. The positive rationals are those greater than 0, and the negative rationals are those less than 0.

The formal definition is that a **real number** is a **cut** of rational numbers, i.e., a subset of rational numbers that is neither $\mathbb{Q}$ nor the empty set, has no largest element, and contains all rational numbers less than any rational that it contains. The set of cuts, i.e., the set of real numbers, is denoted by $\mathbb{R}$. The idea of the construction is as follows: Each rational number q determines a cut q^*, namely the set of all rationals less than q. Under the identification of $\mathbb{Q}$ with a subset of $\mathbb{R}$, the cut defining a real number consists of all rational numbers less than the given real number.

The set of cuts gets a natural ordering, given by inclusion. In place of $\subseteq$, we write $\leq$. For any two cuts r and s, we have $r \leq s$ or $s \leq r$, and if both occur, then $r = s$. We can then define $<$, $\geq$, and $>$ in the expected way. The positive cuts r are those with $0^* < r$, and the negative cuts are those with $r < 0^*$.

Once cuts and their ordering are in place, one can go about defining the usual operations of arithmetic and proving that $\mathbb{R}$ with these operations satisfies the familiar associative, commutative, and distributive laws, and that these interact with inequalities in the usual ways. The definitions of addition and subtraction are easy: the sum or difference of two cuts is simply the set of sums or differences of the rationals from the respective cuts. For multiplication and reciprocals one has to take signs into account. For example the product of two positive cuts consists of all products of positive rationals from the two cuts, as well as 0 and all negative rationals. After these definitions and the proofs of the usual arithmetic operations are complete, it is customary to write 0 and 1 in place of 0^* and 1^*.

This much allows us to define n^{th} roots. The following proposition gives the precise details.

Proposition. If r is a positive real number and n is a positive integer, then there exists a unique positive real number s such that $s^n = r$.

REMARK. In the terminology and notation introduced in Section I.3, the polynomial $X^n - r$ in $\mathbb{R}[X]$ has a unique positive root if r is positive in $\mathbb{R}$.

SKETCH OF PROOF. Let s consist of all positive rationals q such that $q^n < r$, together with all rationals ≤ 0. One checks that s is a cut and that $s^n = r$. This proves existence. For uniqueness any positive cut s' with $(s')^n = r$ must contain exactly the same rationals and hence must equal s. □

To make efficient use of cuts in connection with arithmetic and algebra, one needs to develop a certain amount of real-variable theory. This theory will not be developed in any detail here; let us be content with a sketch, giving a proof of the one specific result that we shall need.[5]

The first step in the process is to observe that any nonempty subset of reals with an upper bound has a least upper bound (the **supremum**, written as sup). This is proved by taking the union of the cuts for each of the given real numbers and showing that the result is a cut. Similarly any nonempty subset of reals with a lower bound has a greatest lower bound (the **infimum**, written as inf). This property follows by applying the least-upper-bound property to the negatives of the given reals and then taking the negative of the resulting least upper bound.

Meanwhile, we can introduce sequences of real numbers and convergence of sequences in the usual way. In terms of convergence, the key property of sequences of real numbers is given by the Bolzano–Weierstrass Theorem: any bounded sequence has a convergent subsequence. In fact, if the given bounded sequence is $\{s_n\}$, it can be shown that there is a subsequence convergent to the greatest lower bound over m of the least upper bound for $k \geq m$ of the numbers s_k.

Next one introduces continuity of functions in the usual way. The Bolzano–Weierstrass Theorem may readily be used to prove that any continuous real-valued function on a closed bounded interval takes on its maximum and minimum values. With a little more effort the Bolzano–Weierstrass Theorem may be used also to show that any continuous real-valued function on a closed bounded interval is uniformly continuous. That brings us to the theorem that we shall use in developing basic algebra.

Theorem (Intermediate Value Theorem). Let $a < b$ be real numbers, and let $f : [a, b] \to \mathbb{R}$ be continuous. Then f, in the interval $[a, b]$, takes on all values between $f(a)$ and $f(b)$.

PROOF. Let $f(a) = \alpha$ and $f(b) = \beta$, and let γ be between α and β. We may assume that γ is in fact strictly between α and β. Possibly by replacing f by $-f$, we may assume that also $\alpha < \beta$. Let

$$A = \{x \in [a, b] \mid f(x) \leq \gamma\} \qquad \text{and} \qquad B = \{x \in [a, b] \mid f(x) \geq \gamma\}.$$

These sets are nonempty since a is in A and b is in B, and f is bounded since any continuous function on a closed bounded interval takes on finite maximum and minimum values. Thus the numbers $\gamma_1 = \sup\{f(x) \mid x \in A\}$ and $\gamma_2 = \inf\{f(x) \mid x \in B\}$ are well defined and have $\gamma_1 \leq \gamma \leq \gamma_2$.

[5] Details of the omitted steps may be found, for example, in Section I.1 of the author's book *Basic Real Analysis*.

If $\gamma_1 = \gamma$, then we can find a sequence $\{x_n\}$ in A such that $f(x_n)$ converges to γ. Using the Bolzano–Weierstrass Theorem, we can find a convergent subsequence $\{x_{n_k}\}$ of $\{x_n\}$, say with limit x_0. By continuity of f, $\{f(x_{n_k})\}$ converges to $f(x_0)$. Then $f(x_0) = \gamma_1 = \gamma$, and we are done. Arguing by contradiction, we may therefore assume that $\gamma_1 < \gamma$. Similarly we may assume that $\gamma < \gamma_2$, but we do not need to do so.

Let $\epsilon = \gamma_2 - \gamma_1$, and choose, since the continuous function f is necessarily uniformly continuous, $\delta > 0$ such that $|x_1 - x_2| < \delta$ implies $|f(x_1) - f(x_2)| < \epsilon$ whenever x_1 and x_2 both lie in $[a, b]$. Then choose an integer n such that $2^{-n}(b-a) < \delta$, and consider the value of f at the points $p_k = a + k2^{-n}(b-a)$ for $0 \le k \le 2^n$. Since $p_{k+1} - p_k = 2^{-n}(b-a) < \delta$, we have $|f(p_{k+1}) - f(p_k)| < \epsilon = \gamma_2 - \gamma_1$. Consequently if $f(p_k) \le \gamma_1$, then

$$f(p_{k+1}) \le f(p_k) + |f(p_{k+1}) - f(p_k)| < \gamma_1 + (\gamma_2 - \gamma_1) = \gamma_2,$$

and hence $f(p_{k+1}) \le \gamma_1$. Now $f(p_0) = f(a) = \alpha \le \gamma_1$. Thus induction shows that $f(p_k) \le \gamma_1$ for all $k \le 2^n$. However, for $k = 2^n$, we have $p_{2^n} = b$. Hence $f(b) = \beta \ge \gamma > \gamma_1$, and we have arrived at a contradiction. □

A4. Complex Numbers

Complex numbers are taken as known, and this section reviews their notation and basic properties.

Briefly, the system $\mathbb{C}$ of complex numbers is a two-dimensional vector space over $\mathbb{R}$ with a distinguished basis $\{1, i\}$ and a multiplication defined initially by $11 = 1$, $1i = i1 = i$, and $ii = -1$. Elements may then be written as $a + bi$ or $a + ib$ with a and b in $\mathbb{R}$; here a is an abbreviation for $a1$. The multiplication is extended to all of $\mathbb{C}$ so that the distributive laws hold, i.e., so that $(a+bi)(c+di)$ can be expanded in the expected way. The multiplication is associative and commutative, the element 1 acts as a multiplicative identity, and every nonzero element has a multiplicative inverse: $(a + bi)\big(\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\big) = 1$.

Complex conjugation is indicated by a bar: the conjugate of $a + bi$ is $a - bi$ if a and b are real, and we write $\overline{a + bi} = a - bi$. Then we have $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{rz} = r\bar{z}$ if r is real, and $\overline{zw} = \bar{z}\bar{w}$.

The **real** and **imaginary parts** of $z = a + bi$ are $\operatorname{Re} z = a$ and $\operatorname{Im} z = b$. These may be computed as $\operatorname{Re} z = \frac{1}{2}(z + \bar{z})$ and $\operatorname{Im} z = -\frac{i}{2}(z - \bar{z})$.

The **absolute value** function of $z = a + bi$ is given by $|z| = \sqrt{a^2 + b^2}$, and this satisfies $|z|^2 = z\bar{z}$. It has the simple properties that $|\bar{z}| = |z|$, $|\operatorname{Re} z| \le |z|$, and $|\operatorname{Im} z| \le |z|$. In addition, it satisfies

$$|zw| = |z||w|$$

because $$|zw|^2 = zw\overline{zw} = zw\bar{z}\bar{w} = z\bar{z}w\bar{w} = |z|^2|w|^2,$$

and it satisfies the **triangle inequality**

$$|z+w| \le |z| + |w|$$

because
$$\begin{aligned} |z+w|^2 &= (z+w)\overline{(z+w)} = z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\ &= |z|^2 + 2\,\mathrm{Re}(z\bar{w}) + |w|^2 \le |z|^2 + 2|z\bar{w}| + |w|^2 \\ &= |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2. \end{aligned}$$

A5. Partial Orderings and Zorn's Lemma

A **partial ordering** on a set S is a relation between S and itself, i.e., a subset of $S \times S$, satisfying two properties. We define the expression $a \le b$ to mean that the ordered pair (a, b) is a member of the relation, and we say that "$\le$" is the partial ordering. The properties are

(i) $a \le a$ for all a in S, i.e., $\le$ is **reflexive**,

(ii) $a \le b$ and $b \le c$ together imply $a \le c$ whenever a, b, and c are in S, i.e., $\le$ is **transitive**.

An example of such an S is any set of subsets of a set X, with $\le$ taken to be inclusion $\subseteq$. This particular partial ordering has a third property of interest, namely

(iii) $a \le b$ and $b \le a$ with a and b in S imply $a = b$.

However, the validity of (iii) has no bearing on Zorn's Lemma below. A partial ordering is said to be a **total ordering** or **simple ordering** if (iii) holds and also

(iv) any a and b in S have $a \le b$ or $b \le a$ or both.

For the sake of a result to be proved at the end of the section, let us interpolate one further definition: a totally ordered set is said to be **well ordered** if every nonempty subset has a least element, i.e., if each nonempty subset contains an element a such that $a \le b$ for all b in the subset.

A **chain** in a partially ordered set S is a totally ordered subset. An **upper bound** for a chain T is an element u in S such that $c \le u$ for all c in T. A **maximal element** in S is an element m such that whenever $m \le a$ for some a in S, then $a \le m$. (If (iii) holds, we can conclude in this case that $m = a$.)

Zorn's Lemma. If S is a nonempty partially ordered set in which every chain has an upper bound, then S has a maximal element.

REMARKS. Zorn's Lemma will be proved below using the Axiom of Choice, which was stated in Section A1. It is an easy exercise to see, conversely, that Zorn's Lemma implies the Axiom of Choice. It is customary with many mathematical writers to mention Zorn's Lemma each time it is invoked, even though most writers nowadays do not ordinarily acknowledge uses of the Axiom of Choice. Before coming to the proof, we give an example of how Zorn's Lemma is used. This example uses vector spaces and is expanded upon in Section II.9.

EXAMPLE. Zorn's Lemma gives a quick proof that any real vector space V has a basis. In fact, let S be the set of all linearly independent subsets of V, and order S by inclusion upward as in the example above of a partial ordering. The set S is nonempty because $\varnothing$ is a linearly independent subset of V. Let T be a chain in S, and let u be the union of the members of T. If t is in T, we certainly have $t \subseteq u$. Let us see that u is linearly independent. For u to be dependent would mean that there are vectors $x_1, \dots, x_n$ in u with $r_1x_1 + \cdots + r_nx_n = 0$ for some system of real numbers not all 0. Let x_j be in the member t_j of the chain T. Since $t_1 \subseteq t_2$ or $t_2 \subseteq t_1$, x_1 and x_2 are both in t_1 or both in t_2. To keep the notation neutral, say they are both in t_2'. Since $t_2' \subseteq t_3$ or $t_3 \subseteq t_2'$, all of x_1, x_2, x_3 are in t_2' or they are all in t_3. Say they are both in t_3'. Continuing in this way, we arrive at one of the sets $t_1, \dots, t_n$, say t_n', such that all of $x_1, \dots, x_n$ are all in t_n'. The members of t_n' are linearly independent by assumption, and we obtain the contradiction $r_1 = \cdots = r_n = 0$. We conclude that the chain T has an upper bound in S. By Zorn's Lemma, S has a maximal element, say m. If m is not a basis, it fails to span. If a vector x is not in its span, it is routine to see that $m \cup \{x\}$ is linearly independent and properly contains m, in contradiction to the maximality of m. We conclude that m is a basis.

We now begin the proof of Zorn's Lemma. If T is a chain in a partially ordered set S, then an upper bound u_0 for T is a **least upper bound** for T if $u_0 \le u$ for all upper bounds of T. If (iii) holds in S, then there can be at most one least upper bound for T. In fact, if u_0 and u_0' are least upper bounds, then $u_0 \le u_0'$ since u_0 is a least upper bound, and $u_0' \le u_0$ since u_0' is a least upper bound; by (iii), $u_0 = u_0'$. The proof follows that in Dunford–Schwartz's *Linear Operators I.*

Lemma. Let X be a nonempty partially ordered set such that (iii) holds, and write $\le$ for the partial ordering. Suppose that X has the additional property that each nonempty chain in X has a least upper bound in X. If $f : X \to X$ is a function such that $x \le f(x)$ for all x in X, then there exists an x_0 in X with $f(x_0) = x_0$.

PROOF. A nonempty subset E of X will be called *admissible* for purposes of this proof if $f(E) \subseteq E$ and if the least upper bound of each nonempty chain in E, which exists in X by assumption, actually lies in E. By assumption, X is an admissible subset of X. If x is in X, then the intersection of admissible subsets of X containing x is admissible. Let A_x be the intersection of all admissible subsets of X containing x. This is admissible, and since the set of all y in X with $x \le y$ is admissible and contains x, it follows that $x \le y$ for all $y \in A_x$. By hypothesis, X is nonempty. Fix an element a in X, and let $A = A_a$. The main step will be to prove that A is a chain.

To do so, consider the subset C of members x of A with the property that there is a nonempty chain C_x in A containing a and x such that

- $a \le y \le x$ for all y in C_x,
- $f(C_x - \{x\}) \subseteq C_x$, and
- the least upper bound of any nonempty subchain of C_x is in C_x.

The element a is in C because we can take $C_a = \{a\}$. If x is in C, so that C_x exists, let us use the bulleted properties to see that

$$A = A_x \cup C_x. \qquad (*)$$

We have $A \supseteq C_x$ by definition; also $A \cap A_x$ is an admissible set containing x and hence containing A, and thus $A \supseteq A_x$. Therefore $A \supseteq A_x \cup C_x$. For the reverse inclusion it is enough to prove that $A_x \cup C_x$ is an admissible subset of X containing a. The element a is in C_x, and thus a is in $A_x \cup C_x$. For the admissibility we have to show that $f(A_x \cup C_x) \subseteq A_x \cup C_x$ and that the least upper bound of any nonempty chain in $A_x \cup C_x$ lies in $A_x \cup C_x$. Since x lies in A_x, $A_x \cup C_x = A_x \cup (C_x - \{x\})$ and $f(A_x \cup C_x) = f(A_x) \cup f(C_x - \{x\}) \subseteq A_x \cup C_x$, the inclusion following from the admissibility of A and the second bulleted property of C_x.

To complete the proof of $(*)$, take a nonempty chain in $A_x \cup C_x$, and let u be its least upper bound in X; it is enough to show that u is in $A_x \cup C_x$. The element u is necessarily in A since A is admissible. Observe that

$$y \le x \quad \text{and} \quad x \le z \qquad \text{whenever } y \text{ is in } C_x \text{ and } z \text{ is in } A_x. \qquad (**)$$

If the chain has at least one member in A_x, then $(**)$ implies that $x \le u$, and hence the set of members of the chain that lie in A_x forms a nonempty chain in A_x with least upper bound u. Since A_x is admissible, u is in A_x. Otherwise the chain has all its members in C_x, and then u is in C_x by the third bulleted property of C_x.

This completes the proof of $(*)$. Let us now prove that if C_x and $C_{x'}$ exist with $x \le x'$ and $x \ne x'$, then

$$C_x \subseteq C_{x'}. \qquad (\dagger)$$

In fact, application of $(*)$ to x' gives $A = A_{x'} \cup C_{x'}$. Intersecting both sides with C_x shows that $C_x = (C_x \cap A_{x'}) \cup (C_x \cap C_{x'})$. On the right side, the first member is empty by $(**)$, and thus $C_x = C_x \cap C_{x'}$. This proves $(\dagger)$.

Let C be the set of all members x of A for which C_x exists. We have seen that a is in C. If we apply $(*)$ and $(**)$ first to a member x of C and then to a member x' of C, we see that either $x \le x'$ or $x' \le x$. That is, C is a chain.

Let us see that $f(C) \subseteq C$. If x is in C, then the set $D = C_x \cup \{f(x)\}$ certainly has a as a member. The second bulleted property of C_x shows that f carries $C_x - \{x\}$ into D, and also f carries x into D. Thus f carries $D - \{f(x)\}$ into D, and D satisfies the second bulleted property of $C_{f(x)}$. If $\{x_\alpha\}$ is a chain in D with least upper bound u, there are two possibilities. Either u is $f(x)$, which is in D by construction, or u is in C, which contains the least upper bound of any nonempty chain in it. Thus u is in D, D satisfies the third bulleted property of $C_{f(x)}$, and $C_{f(x)}$ exists. In other words, $f(x)$ is in C, and $f(C) \subseteq C$.

Finally let us see that the least upper bound u of an arbitrary chain $\{x_\alpha\}$ in C, which exists in X by assumption, is a member of C. If $x_\alpha = u$ for some α, then $C_u = C_{x_\alpha}$ exists, and u is in C. So assume that $x_\alpha \neq u$ for all α. Our candidate for C_u will be $D = (\bigcup_\alpha C_{x_\alpha}) \cup \{u\}$. This certainly contains a. We check that D satisfies the second bulleted property of C_u. For each α, we can find a β with $x_\alpha \leq x_\beta$ and $x_\alpha \neq x_\beta$, since u is the least upper bound of all the x's. Then (†) gives $C_{x_\alpha} \subseteq C_{x_\beta} - \{x_\beta\}$, and $f(C_{x_\alpha}) \subseteq f(C_{x_\beta} - \{x_\beta\}) \subseteq C_{x_\beta} \subseteq D$. Taking the union over α shows that D satisfies the second bulleted property of C_u.

To see that D satisfies the third bulleted property of C_u, let v be the least upper bound in A of a chain $\{y_\beta\}$ in C_u. If $v \neq u$, then v cannot be an upper bound of $\{x_\alpha\}$. So we can choose some x_{α_0} such that $v \leq x_{\alpha_0}$. Each y_β is $\leq v$, and thus each y_β is $\leq x_{\alpha_0}$. Referring to $(*)$, we see that all y_β's lie in $C_{x_{\alpha_0}}$. By the third bulleted property of $C_{x_{\alpha_0}}$, v is in $C_{x_{\alpha_0}}$. Thus v is in D, and D satisfies the third bulleted property of C_u. Consequently the least upper bound u of an arbitrary chain in C lies in C.

In short, C is an admissible set containing a, and it also is a chain. Since A is a minimal admissible set containing a, $C = A$ and also A is a chain. Let u be the least upper bound of A. We have seen that $f(A) \subseteq A$, and thus $f(u) \leq u$. On the other hand, $u \leq f(u)$ by the defining property of f. Therefore $f(u) = u$, and the proof is complete.

PROOF OF ZORN'S LEMMA. Let S be a partially ordered set, with partial ordering $\leq$, in which every chain has an upper bound. Let X be the partially ordered system, ordered by inclusion upward $\subseteq$, of nonempty chains[6] in S. The partially ordered system X, being given by ordinary inclusion, satisfies property (iii). A nonempty chain C in X is a nested system of chains c_α of S, and $\bigcup_\alpha c_\alpha$ is a chain in S that is a least upper bound for C. The lemma is therefore applicable to any function $f : X \to X$ such that $c \subseteq f(c)$ for all c in X. We use the lemma to produce a maximal chain in X.

Arguing by contradiction, suppose that no chain within S is maximal under

[6] Here a chain is simply a certain kind of subset of S, and no element of S can occur more than once in it even if (iii) fails for the partial ordering. Thus if $S = \{x, y\}$ with $x \leq y$ and $y \leq x$, then $\{x, y\}$ is in X and in fact is maximal in X.

inclusion. For each nonempty chain c within S, let $f(c)$ be a chain with $c \subseteq f(c)$ and $c \neq f(c)$. (This choice of $f(c)$ for each c is where we use the Axiom of Choice.) The result is a function $f : X \to X$ of the required kind, the lemma says that $f(c) = c$ for some c in X, and we arrive at a contradiction. We conclude that there is some maximal chain c_0 within S.

By assumption in Zorn's Lemma, every nonempty chain within S has an upper bound. Let u_0 be an upper bound for the maximal chain c_0. If u is a member of S with $u_0 \leq u$, then $c_0 \cup \{u\}$ is a chain and maximality implies that $c_0 \cup \{u\} = c_0$. Therefore u is in c_0, and $u \leq u_0$. This is the condition that u_0 is a maximal element of S. □

Corollary (Zermelo's Well-Ordering Theorem). Every set has a well ordering.

PROOF. Let S be a set, and let $\mathcal{E}$ be the family of all pairs $(E, \leq_E)$ such that E is a subset of S and $\leq_E$ is a well ordering of E. The family $\mathcal{E}$ is nonempty since $(\varnothing, \varnothing)$ is a member of it. We partially order $\mathcal{E}$ by a notion of "inclusion as an initial segment," saying that $(E, \leq_E) \leq (F, \leq_F)$ if

(i) $E \subseteq F$,
(ii) a and b in E with $a \leq_E b$ implies $a \leq_F b$,
(iii) a in E and b in F but not E together imply $a \leq_F b$.

In preparation for applying Zorn's Lemma, let $\mathcal{C} = \{(E_\alpha, \leq_\alpha)\}$ be a chain in $\mathcal{E}$, with the α's running through some set I. Define $E_0 = \bigcup_\alpha E_\alpha$ and define $\leq_0$ as follows: If e_1 and e_2 are in E_0, let e_1 be in E_{α_1} with α_1 in I, and let e_2 be in E_{α_2} with α_2 in I. Since $\mathcal{C}$ is a chain, we may assume without loss of generality that $(E_{\alpha_1}, \leq_{\alpha_1}) \leq (E_{\alpha_2}, \leq_{\alpha_2})$, so that $E_{\alpha_1} \subseteq E_{\alpha_2}$ in particular. Then e_1 and e_2 are both in E_{α_2} and we define $e_1 \leq_0 e_2$ if $e_1 \leq_{\alpha_2} e_2$, and $e_2 \leq_0 e_1$ if $e_2 \leq_{\alpha_2} e_1$. Because of (i) and (ii) above, the result is well defined independently of the choice of α_1 and α_2. Similar reasoning shows that $\leq_0$ is a total ordering of E_0. If we can prove that $\leq_0$ is a well ordering, then $(E_0, \leq_0)$ is evidently an upper bound in $\mathcal{E}$ for the chain $\mathcal{C}$, and Zorn's Lemma is applicable.

Now suppose that F is a nonempty subset of E_0. Pick an element of F, and let E_{α_0} be a set in the chain that contains it. Since $(E_{\alpha_0}, \leq_{\alpha_0})$ is well ordered and $F \cap E_{\alpha_0}$ is nonempty, $F \cap E_{\alpha_0}$ contains a least element f_0 relative to $\leq_{\alpha_0}$. We show that $f_0 \leq_0 f$ for all f in F. In fact, if f is given, there are two possibilities. One is that f is in E_{α_0}; in this case, the consistency of $\leq_0$ with $\leq_{\alpha_0}$ forces $f_0 \leq_0 f$. The other is that f is not in E_{α_0} but is in some E_{α_1}. Since $\mathcal{C}$ is a chain and $E_{\alpha_1} \subseteq E_{\alpha_0}$ fails, we must have $(E_{\alpha_0}, \leq_{\alpha_0}) \leq (E_{\alpha_1}, \leq_{\alpha_1})$. Then f is in E_{α_1} but not E_{α_0}, and property (iii) above says that $f_0 \leq_{\alpha_1} f$. By the consistency of the orderings, $f_0 \leq_0 f$. Hence f_0 is a least element in F, and E_0 is well ordered.

Application of Zorn's Lemma produces a maximal element $(E, \leq_E)$ of $\mathcal{E}$. If E were a proper subset of S, we could adjoin to E a member s of S not in E and define every element e of E to be $\leq s$. The result would contradict maximality. Therefore $E = S$, and S has been well ordered. $\square$

A6. Cardinality

Two sets A and B are said to have the same **cardinality**, written $\operatorname{card} A = \operatorname{card} B$, if there exists a one-one function from A onto B. On any set $\mathcal{A}$ of sets, "having the same cardinality" is plainly an equivalence relation and therefore partitions $\mathcal{A}$ into disjoint equivalence classes, the sets in each class having the same cardinality. The question of what constitutes cardinality (or a "cardinal number") in its own right is one that is addressed in set theory but that we do not need to address carefully here; the idea is that each equivalence class under "having the same cardinality" has a distinguished representative, and the **cardinal number** is defined to be that representative. We write $\operatorname{card} A$ for the cardinal number of a set A.

Having addressed equality, we now introduce a partial ordering, saying that $\operatorname{card} A \leq \operatorname{card} B$ if there is a one-one function from A into B. The first result below is that $\operatorname{card} A \leq \operatorname{card} B$ and $\operatorname{card} B \leq \operatorname{card} A$ together imply $\operatorname{card} A = \operatorname{card} B$.

Proposition (Schroeder–Bernstein Theorem). If A and B are sets such that there exist one-one functions $f : A \to B$ and $g : B \to A$, then A and B have the same cardinality.

PROOF. Define the function $g^{-1} : \operatorname{image} g \to A$ by $g^{-1}(g(a)) = a$; this definition makes sense since g is one-one. Write $(g \circ f)^{(n)}$ for the composition of $g \circ f$ with itself n times, and define $(f \circ g)^{(n)}$ similarly. Define subsets A_n and A'_n of A and subsets B_n and B'_n for $n \geq 0$ by

$$\begin{aligned}
A_n &= \operatorname{image}((g \circ f)^{(n)}) - \operatorname{image}((g \circ f)^{(n)} \circ g),\\
A'_n &= \operatorname{image}((g \circ f)^{(n)} \circ g) - \operatorname{image}((g \circ f)^{(n+1)}),\\
B_n &= \operatorname{image}((f \circ g)^{(n)}) - \operatorname{image}((f \circ g)^{(n)} \circ f),\\
B'_n &= \operatorname{image}((f \circ g)^{(n)} \circ f) - \operatorname{image}((f \circ g)^{(n+1)}),
\end{aligned}$$

and let

$$A_\infty = \bigcap_{n=0}^{\infty} \operatorname{image}((g \circ f)^{(n)}) \qquad \text{and} \qquad B_\infty = \bigcap_{n=0}^{\infty} \operatorname{image}((f \circ g)^{(n)}).$$

Then we have

$$A = A_\infty \cup \bigcup_{n=0}^{\infty} A_n \cup \bigcup_{n=0}^{\infty} A'_n \qquad \text{and} \qquad B = B_\infty \cup \bigcup_{n=0}^{\infty} B_n \cup \bigcup_{n=0}^{\infty} B'_n,$$

with both unions disjoint.

Let us prove that f carries A_n one-one onto B'_n. If a is in A_n, then $a = (g \circ f)^{(n)}(x)$ for some $x \in A$ and a is not of the form $(g \circ f)^{(n)}(g(y))$ with $y \in B$. Applying f, we obtain $f(a) = (f \circ ((g \circ f)^{(n)})(x) = (f \circ g)^{(n)}(f(x))$, so that $f(a)$ is in the image of $((f \circ g)^{(n)} \circ f)$. Meanwhile, if $f(a)$ is in the image of $(f \circ g)^{(n+1)}$, then $f(a) = (f \circ g)^{(n+1)}(y) = f((g \circ f)^{(n)}(g(y)))$ for some $y \in B$. Since f is one-one, we can cancel the f on the outside and obtain $a = (g \circ f)^{(n)}(g(y))$, in contradiction to the fact that a is in A_n. Thus f carries A_n into B'_n, and it is certainly one-one. To see that $f(A_n)$ contains all of B'_n, let $b \in B'_n$ be given. Then $b = (f \circ g)^{(n)}(f(x))$ for some $x \in A$ and b is not of the form $(f \circ g)^{(n+1)}(y)$ with $y \in B$. Hence $b = f((g \circ f)^{(n)}(x))$, i.e., $b = f(a)$ with $a = (g \circ f)^{(n)}(x)$. If this element a were in the image of $(g \circ f)^{(n)} \circ g$, we could write $a = (g \circ f)^{(n)}(g(y))$ for some $y \in B$, and then we would have $b = f(a) = f((g \circ f)^{(n)}(g(y))) = (f \circ g)^{(n+1)}(y)$, contradiction. Thus a is in A_n, and f carries A_n one-one onto B'_n.

Similarly g carries B_n one-one onto A'_n. Since A'_n is in the image of g, we can apply g^{-1} to it and see that g^{-1} carries A'_n one-one onto B_n.

The same kind of reasoning as above shows that f carries A_∞ one-one onto B_∞. In summary, f carries each A_n one-one onto B'_n and carries A_∞ one-one onto B_∞, while g^{-1} carries each A'_n one-one onto B_n. Then the function

$$h = \begin{cases} f & \text{on } A_\infty \text{ and each } A_n, \\ g^{-1} & \text{on each } A'_n, \end{cases}$$

carries A one-one onto B. □

Next we show that any two sets A and B have comparable cardinalities in the sense that either card $A \le$ card B or card $B \le$ card A.

Proposition. If A and B are two sets, then either there is a one-one function from A into B or there is a one-one function from B into A.

PROOF. Consider the set S of all one-one functions $f : E \to B$ with $E \subseteq A$, the empty function with $E = \varnothing$ being one such. Each such function is a certain subset of $A \times B$. If we order S by inclusion upward, then the union of the members of any chain is an upper bound for the chain. By Zorn's Lemma let $G : E_0 \to B$ be a maximal one-one function of this kind, and let F_0 be the image of G. If $E_0 = A$, then G is a one-one function from A into B. If $F_0 = B$, then G^{-1} is a one-one function from B into A. If neither of these things happens, then there exist $x_0 \in A - E_0$ and y_0 in $B - F_0$, and the function $\widetilde{G}$ equal to G on E_0 and having $\widetilde{G}(x_0) = y_0$ extends G and is still one-one; thus it contradicts the maximality of G. □

Corollary. If E is an infinite set, then E has a countably infinite subset.

PROOF. The proposition shows that either there is a one-one function from the set of positive integers into E, in which case we are done, or there is a one-one function from E into the set of positive integers. In the latter case the image cannot be finite since E is assumed infinite. Then the image must be an infinite subset of the positive integers. This set can be enumerated and is therefore countably infinite. Thus E is countably infinite. □

Cantor's proof that there exist uncountable sets, done with a diagonal argument, in fact showed how to start from any set A and construct a set with strictly larger cardinality.

Proposition (Cantor). If A is a set and 2^A denotes the set of all subsets of A, then card 2^A is strictly larger than card A.

PROOF. The map $x \mapsto \{x\}$ is a one-one function from A into 2^A. If we are given a one-one function $F : A \to 2^A$, let E be the set of all x in A such that x is not in $F(x)$. If we define $E = F(x_0)$, then $x_0 \in E$ implies $x_0 \notin F(x_0) = E$, while $x_0 \notin E$ implies $x \in F(x_0) = E$. We have a contradiction in any case, and hence E cannot be of the form $F(x_0)$. We conclude that F cannot be onto 2^A. □

Proposition. If E is an infinite set, then E is the disjoint union of sets that are each countably infinite.

PROOF. Let $\mathcal{S}$ be the set of all disjoint unions of countably infinite subsets of E. If $A = \bigcup_\alpha A_\alpha$ and $B = \bigcup_\beta B_\beta$ are members of $\mathcal{S}$, say that $A \leq B$ if each A_α is some B_β. The result is a partial ordering on $\mathcal{S}$. If $\mathcal{U}$ is a chain in $\mathcal{S}$, then the collection C of all countably infinite sets that are U_α's in some member of $\mathcal{U}$ is a collection of countably infinite subsets of E that contains each member of $\mathcal{U}$. If U_α and U_β are distinct members of C, then U_α and U_β must both be in some member of $\mathcal{U}$ and hence must be disjoint. Thus C is an upper bound for $\mathcal{U}$. Also, the empty union is a member of $\mathcal{S}$. By Zorn's Lemma, $\mathcal{S}$ has a maximal element M. Let F be the union of the members of M. If $E - F$ were to be infinite, then the corollary above would show that $E - F$ has a countably infinite subset Z, and $M \cup \{Z\}$ would contradict the maximality of M. Thus $E - F$ is finite. Since E is infinite, the corollary shows that E contains at least one countably infinite subset. Thus M has some member T. The set $T' = T \cup (E - F)$ is countably infinite, and $(M - \{T\}) \cup T'$ is the required decomposition of E as the disjoint union of countably infinite sets. □

Corollary. Let S and E be nonempty sets with S infinite, and suppose that to each element s of S is associated a countable subset E_x of E in such a way that $E = \bigcup_{s \in S} E_s$. Then card $E \leq$ card S.

PROOF. The proposition allows us to write S as the disjoint union of countably infinite sets. If U is one of these sets, then $E_U = \bigcup_{s \in U} E_s$ is countable, being the countable union of countable sets. Therefore there exists a function from U onto E_U. The union of these functions, as U varies, yields a function f from S onto $\bigcup E_U = E$. Applying the Axiom of Choice, we can select, for each $e \in E$, an element $s \in f^{-1}(\{e\})$ and call it $g(e)$. The result is a one-one function g from E into S, and consequently $\operatorname{card} E \leq \operatorname{card} S$. □

Addition is well defined for cardinals: the **sum of two cardinal numbers** is defined to be the cardinality of the disjoint union of the two sets in question. If at least one of the two cardinals is infinite, the sum equals the larger of the two, as an immediate consequence of the above corollary.