Mathematical Literacy for Humanists

Mathematical Literacy for Humanists

Herbert Gintis

xxxxxxxxx xxxxxxxxxx Press
xxxxxxxxx and xxxxxx

Published by ...
Library of Congress Cataloging-in-Publication Data
Gintis, Herbert
Mathematical Literacy for Humanists/
Herbert Gintis
p. cm.
Includes bibliographical references and index.
ISBN ...(hardcover: alk. paper)
HB...

xxxxxxxxxx
British Library Cataloging-in-Publication Data is available
The publisher would like to acknowledge the author of this volume for providing the
camera-ready copy from which this book was printed
This book has been composed in Times and Mathtime by the author
Printed on acid-free paper.
Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

This book is dedicated to

Contents

Preface

The eternal mystery of the world is its comprehensibility.

Albert Einstein

This book is for people who believe that those who study human society using formal mathematical models might have something to say to them, but for whom the mathematical formalism is a foreign language that they do not understand. More generally it is for anyone who is curious about the nature of mathematical and logical thought and their relationship to the universe.

Often mathematics is justified by its being useful, and it is. But useful things can be beautiful, and things can be beautiful without be useful at all. This is something the humanists have taught us. I stress in this book that mathematics is beautiful even if we don't care a whit about its usefulness. Mathematics is beautiful in the same way that music, dance, and literature are beautiful. Mathematics may even be more beautiful because it takes a lot of work to appreciate it. A *lot* of work. If you get through this book, you will have done a lot of work. But, on the other hand, you will have acquired the capacity to envision worlds you never even dreamed were there. Worlds of logical and algebraic structures.

More times than I care to remember I have heard intelligent people proclaim that they are awful at math, that they hate it, and that they never use it. In so doing, they project an air of imperfectly concealed self-satisfaction. I usually smile and let it pass. I know that these people expect to be admired for their capacity to avoid the less refined of life's activities.

In fact, I do feel sympathy for these friends. I let their judgments on the topic pass without comment, rather than inform them of the multitudinous pleasurable insights their condition precludes their enjoying. Thinking that mathematics is calculating is about as silly as thinking that painting a landscape is like painting a woodshed, or that ballet is aerobic exercise.

This book treats mathematics as a language that fosters certain forms of truthful communication that are difficult to express without specialized symbols. Some mathematicians are fond of saying that anything worth expressing can be expressed in words. Perhaps. But that does not mean any-

thing can be understood in words. Even the simplest mathematical statement would take many thousands of words to write out in full.

This is just the skeleton of the beginning of a text. I would like comments and suggestions, both humanist and mathematical. Please email me at hgintis@comcast.net.

1

Reading Math

1.1 Reading Math

Reading math is not like reading English. In reading a novel, a history book, or the newspaper, you can read a sentence, not understand it perfectly (perhaps there's an ambiguous word, or you're not sure what a pronoun refers to), and yet move on to the next sentence. In reading math, you must understand *every expression perfectly* or you do not understand it at all. Thus, you either understand something like equation (3.9) perfectly, or you don't understand it at all. If the latter is the case, read the expression symbol by symbol until you come to the one that doesn't make sense. Then find out exactly what it means before you go on.

2

The Language of Logic

People are not logical. They are psychological.

Unknown

2.1 The Language of Logic

The term *true* is a *primitive* of logic; i.e., we do not define the term 'true' in terms of more basic terms. The logic used in mathematical discourse has only three primitive terms in addition to 'true'. These are 'not,' 'and,' and 'for all.'

We define "false" as "not true," and we define a *propositional variable* as an entity that can have the value either true or false, but not both. By the way, "true" is a *propositional constant* because, unlike a variable, its value cannot change. The only other propositional constant is "false."

In this chapter, we will use p, q, r, s and so on to represent propositional variables. In general, if p is a propositional variable, we define $\neg p$ to be a propositional variable that is true exactly when p is false. When we assert p, we are saying that p has the value true. From these, we can define all sorts of other logical terms. We when we assert "p and q", we are asserting that both p and q are true. We write this logically as $p \wedge q$. The four terms *true*, *false*, *not*, and *and* are used in logic almost exactly as in natural language communication.

Many other logical terms can be defined in terms of *and* and *not*. We define "p or q", which we write as $p \vee q$, to be a true when either p or q is true, and is false otherwise. We can define this in terms of "not" and "and" as $\neg(\neg p \wedge \neg q)$. we call $\vee$ the *inclusive or* because in natural language "or" can be either inclusive or exclusive. An example of an exclusive or is in the following conversation. Little boy: "I would like Bob and Jim to come to the playground with me." Mother: "This is too many people. You can invite Bob or Jim." In logic and math, we would write "Bob or Jim" in this sentence as $(p_b \vee p_j) \wedge (\neg(p_b \wedge p_j))$, where p_b means "you can invite Bob" and p_j means "you can invite Jim."

Actually, the expression $(p_b \vee p_j) \wedge (\neg(p_b \wedge p_j))$ is fairly typical of what you run into in reading mathematics. At first it looks like a jumble of symbols. But if you look closely, you notice that it is a conjuntion of two expressions, so if you can understand each of the two, you will understand the whole. The first is easy: p_b or p_j. The second is the negation of the conjunction p_b and p_j, so the second term means not both p_b and p_j. You then get that Aha! feeling: the expression means p_b or p_j, but not both. You may wonder why the writer did not just use words. The reason is that in a more complex argument, the verbal translation would be much harder to understand than the mathematical.

We say "p implies q," which we write $p \to q$, if q is true or p is false; i.e. $p \to q$ has the same meaning as $(\neg p) \vee q$. This definition of implication has the nice property that it justifies the most important form of logical inference, called *modus ponens*. According to modus ponens, if p is true and if $p \to q$ is true, then q must be true. However, $\to$ has some unfortunate idiosyncracies that distance logical implication (which is often called *material implication*) from the notion of logical entailment in everyday language and thought. For instance, if q is true, then $p \to q$ is true, no matter what p is. So for instance, "swans are white" $\to$ "cigarettes cause cancer" is a true implication, but surely cigarettes do not cause cancer *because* swans are white, and cigarettes would still cause cancer if a sudden miracle turned all swans purple. In the same vein, "Göethe was two feet tall" implies both "$2 + 3 = 5$" and "$2 + 3 = 23$".

We often translate the material implication $p \to q$ as "if p then q," although again the formal definition of material implication clashes with everyday usage. For instance, if Mommy says "If you eat all your vegetables, then you will be allowed go out and play after dinner," and if little Joey does not eat his vegetables, he may still go out and play without violating Mommy's assertion as a material implication. In fact, Mommy means "*Only* if you eat your vegetables, will you be allowed to go out and play after dinner." There is no ambiguity in everyday discourse in dropping the "only," since the sentence would be silly otherwise.

Formal logic, however, does not know from silly; we write "q only if p" as $(\neg p) \to (\neg q)$ (if p is false, then q must be false). However, if you check the definition, you will see that this expression means the same thing as $q \to p$. So when Mommy says "If p then q" where p means "you eat your vegetables" and q means "you can go out and play," she really means, in terms of mathematical logic, "if q then p".

We can combine 'if' and 'only if' by using the phrase "p if and only if q", which means p and q have the same truth-value, or equivalently $(p \to q) \wedge (q \to p)$. We can abbreviate this as $p \leftrightarrow q$, or $p \equiv q$.

2.2 Formal Propositional Logic

Suppose we have a set of propositional variables p, q, r, s, and so on, which we term *atomic* propositions. We use the *logical connectives* and propositional constants that we defined in the previous section, as follows:

$p \wedge q$	p and q
$p \vee q$	p or q
$\neg p$	not p
$p \to q$	p implies q
$p \leftrightarrow q$	p if and only if q
$\bot$	false
$\top$	true

We call the expressions resulting from linking together propositional variables and constants *compound propositions*. We define a *string* to be any concatenation of propositional variables, logical connectives, propositional constants, and parenthesis of finite length. For instance,

$$pp\vee) \leftrightarrow q((\bot rs \to)$$

is a string (although it doesn't mean anything).

We now define the set of *well-formed propositions* PC to be the smallest set of strings of propositional variables, logical connectives, and propositional constants such that

- The propositional variables p, q, etc. are in PC, as are the propositional constants $\bot$ and $\top$.
- If s and t are in PC, then $(s \wedge t)$, $(s \vee t)$, $(\neg s)$, $(s \to t)$ and $(s \leftrightarrow t)$ are in PC.

Thus, for instance,

$$(((((p \to q)) \wedge p)) \to q) \tag{2.1}$$

is a propositional sentence. This sentence was formed as follows. First, substitute p and q for s and t in $(s \to t)$, giving $(p \to q)$. Second, substitute this expression for s and p for t in $(s \wedge t)$, getting $((p \to q) \wedge p)$, Now substitute this exprression for s and q for t in $(s \to t)$, getting (2.1).

Of course, (2.1) has so many parentheses that it is virtually unreadable. We thus add several conventions that allow us to eliminate useless parentheses. The first is we can always eliminate the outer pair of parentheses in expression s like $((s))$. Applying this twice, this reduces (2.1) to

$$((p \to q) \wedge p) \to q.$$

This is now pretty readable. It says "If p implies q, and if p is true, then q is true. As we have seen, this is the venerable *modus ponens*.

We also assume that $\leftrightarrow$ and $\to$ bind their arguments more tightly that $\vee$ or $\wedge$, so we can write (2.1) as

$$(p \to q \wedge p) \to q.$$

This, however, can easily be confusing, so we often leave in parentheses where we would otherwise be forced to think about which logical connectives bind more tightly than which others.

We also assume that $\neg$ binds more strongly that $\to$ so, for instance, $\neg p \to q$ is really $(\neg p) \to q$, rather than $\neg(p \to q)$.

2.3 Truth Tables

The easiest way to clarify the meaning of these logical connectives is by using *truth tables*. The truth table for $\wedge$ is

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F.

The truth table for $\vee$ is

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F.

This says that $p \vee q$ is true exactly when at least one of p and q is true.

The truth table for $\neg$ is simplest of all:

p	$\neg p$
T	F
F	T.

Thus, $\neg p$ is true exactly when p is false.

The truth table for $\leftrightarrow$ is

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T.

Thus $p \leftrightarrow q$ is true if p and q are either both true or both false.

We say that a well-formed proposition is *true* if its truth-value is true whatever truth-values are assigned to the atomic propositions it contains. Truth tables allow you to determine whether any well-formed proposition is true or false. For example, here is how we show that modus ponens, equation (2.1), is in fact true. We first form the truth table and fill in values for p and q:

p	q	$((p$	$\rightarrow$	$q)$	$\wedge$	$p)$	$\rightarrow$	q
T	T	T		T		T		T
T	F	T		F		T		F
F	T	F		T		F		T
F	F	F		F		F		F

The only thing we can evaluate now is $p \rightarrow q$, which we do, and then erase the p and q on either side of the $\rightarrow$, getting

p	q	$((p$	$\rightarrow$	$q)$	$\wedge$	$p)$	$\rightarrow$	q
T	T		T			T		T
T	F		F			T		F
F	T		T			F		T
F	F		T			F		F

Now we can evaluate the $\wedge$ of the column under the $\rightarrow$ and the column under the p, and put the result under the $\wedge$, thus getting the value of the sub-expression $((p \rightarrow q) \wedge p)$. I erase the two lines that we used to get this result, so we have

p	q	$((p$	$\rightarrow$	$q)$	$\wedge$	$p)$	$\rightarrow$	q
T	T				T			T
T	F				F			F
F	T				F			T
F	F				F			F

Finally, we can evaluate the column under the $\wedge$, and the final q, connected by the $\rightarrow$, and put the result under the final $\rightarrow$, thus getting the value of the whole expression in the column under the final $\rightarrow$. I then erase the two columns we used to get this result, so we have

p	q	$((p$	$\rightarrow$	$q)$	$\wedge$	$p)$	$\rightarrow$	q
T	T						T	
T	F						T	
F	T						T	
F	F						T	

Because the value of the whole expression is true for all truth-value assignments to p and q, we have proven the assertion.

There is actually a second way to prove the assertion without so much work, but it requires a little finesse. We suppose the assertion is false, and derive a contradiction. This is called *proof by contradiction* or *reductio ad absurdum*. So, suppose the assertion is false. An implication $s \rightarrow t$ is false only when s is true and t is false. So, suppose q is false, but $(p \rightarrow q) \wedge p$ is true. A statement $s \wedge t$ is true only if both s and t are true. We thus must have p is true and $p \rightarrow q$ is true. Because q is false, this means p must be false, which is a contradiction, since we have already seen that p must be true. This proves the assertion.

2.4 Exercises in Propositional Logic

A *tautology* is a well-formed proposition that is true no matter what the truth value of the atomic propositions of which it is composed. The following are some tautologies from propositional logic. Prove them using truth tables, and say what they mean in words.

- Modus Ponens: $(p \wedge (p \rightarrow q)) \rightarrow q$;
- Modus Tollens: $(p \rightarrow q) \wedge \neg q) \rightarrow \neg p$;
- $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$;
- $((p \vee q) \wedge \neg p) \rightarrow q$;
- $((p \vee q) \vee r) \leftrightarrow (p \vee (q \vee r))$

- $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$
- $((p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r)) \rightarrow (q \vee s)$;
- $p \wedge q \rightarrow p$
- $p \rightarrow p \vee q$
- $((p \rightarrow q) \wedge (p \rightarrow r)) \rightarrow (p \rightarrow (q \wedge r))$;
- De Morgan's Theorem I: $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
- De Morgan's Theorem II: $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$
- Double Negation: $\neg\neg p \leftrightarrow p$;
- Distributive I: $p \wedge (q \vee r)) \leftrightarrow (p \wedge q) \vee (p \wedge r)$;
- Distributive II: $p \vee (q \wedge r)) \leftrightarrow (p \vee q) \wedge (p \vee r)$;
- Law of Excluded Middle: $p \vee \neg p$.

2.5 Predicate Logic

There are many important things you cannot say using propositional logic. For instance, you cannot say "if an integer is not divisible by 2, then its successor is divisible by 2." This is because the antecedent, "an integer is not divisible by 2," is not a proposition with a truth value. However, let p be the statement "if an integer between 1 and 7 is not divisible by 2, then its successor is divisible by 2." We can express this statement in the propositional calculus as follows. Let $P(n)$ be the sentence "If n is not divisible by 2, then $n + 1$ is divisible by 2." Then we have

$$p \leftrightarrow P(1) \wedge P(2) \wedge P(3) \wedge P(4) \wedge P(5) \wedge P(6) \wedge P(7).$$

The problem appears to be that to express the more general statement that if an integer is not even (divisible by 2), then its successor is even, we need an infinite conjuction, which is not allowed in the propositional calculus, and indeed could not even be written out in the propositional calculus.

The solution is to construct a more powerful logical system called *predicate logic*. We get this system by adding a single new primitive term "for all," as well as some new symbols that we call *variables*, and write x, y, z, and so on, perhaps with subscripts if we are afraid of running out of appropriate letters. Finally, we introduce *predicates* $P(x)$, $Q(x, y)$, $R(x, y, z)$, and so on, which become propositions (i.e., are either true or false) when a real thing is substituted for each "placeholder" variable x, y, or z. For instance, let $P(x)$ be the predicate "if x is an integer and x is not divisible by 2, then $x + 1$ is divisible by 2." We then express our desired assertion by saying "For all x, $P(x)$." We write this in symbols as $(\forall x)P(x)$.

Sometimes rather than writing $(\forall x)(P(x) \rightarrow Q(x))$ we write $(\forall x \in P)(Q(x))$, which reads "for all x in P,$Q(x)$." The symbol $\in$ is a primitive term of *set theory*, which we will cover later. In this case we consider the predicate P to be the set of all things for which $P(x)$.

We can define another basic symbol of predicate logic, "there exists," in terms of "for all." To say that there exists some x such that $P(x)$ means that $\neg P(x)$ is not true for all x, or more simply, $\neg(\forall x)\neg P(x)$. We write "there exists" as $(\exists)$. Thus we have

$$(\exists x)P(x) \leftrightarrow \neg(\forall x)\neg P(x).$$

If you think about it for a bit, you will see that the following is also true:

$$(\forall x)P(x) \leftrightarrow \neg(\exists x)\neg P(x).$$

Note that you can interchange contiguous $\forall$'s and contiguous $\exists$'s and preserve the meaning of the expression, but you cannot interchange a $\forall$ and a $\exists$. For instance, restricting ourselves to variables representing human beings, let $P(x, y)$ mean "x is the father of y." Then $(\forall y)(\exists x)(P(x, y))$ may be true (every human has a father), although $(\exists x)(\forall y)(P(x, y))$ is surely false, since there is no human who is the father of every human.

2.6 Proving Propositions in Predicate Logic

If you can prove that a predicate $P(x)$ is true using the propositional calculus, then $(\forall x)P(x)$ is true in the predicate calculus. For instance, we can prove if $P(x)$ and if $P(x) \rightarrow Q(x, y)$, then $Q(x, y)$, which is Modus Ponens, in the same way as in the propositional calculus, using truth tables. We simply assume $P(x)$ is a new propositional variable rather than interpreting it as a predicate. Moreover, we have the obvious implications $P(x) \rightarrow (\forall x)P(x)$, meaning that if we can prove $P(x)$ without knowing anything about x, then $P(x)$ must be true for all x. Moreover, as long as there exists some x, $P(x) \rightarrow (\exists x)P(x)$.

However, in general it is far harder to prove things in the predicate calculus than in the propositional calculus. That will not worry us, though, because using mathematics as a means of communication frees us from concerning ourselves with how things are proved, just as we can use a telephone if we know which buttons to press when, without knowing anything about electromagnetic theory.

2.7 The Perils of Logic

When Gotlob Frege, perhaps the greatest logician since Aristotle, had just put the finishing touches on the second volume of his masterwork *The Basic Laws of Arithmetic* (1903), he received a letter from the young Bertrand Russell exhibiting a logical contradiction at the heart of elementary set theory. We will deal with Russell's Paradox later, but it is worth stating here that perplexing paradoxes can be found in predicate logic as well. These paradoxes are even more perplexing that Russell's and other paradoxes of set theory because they are much more difficult to avoid.

The most important paradox of predicate logic is the *Liar's Paradox*. In its simplest form, the Liar's Paradox is "This sentence is false." First, you should convince yourself that a sentence like this cannot be part of propositional logic, but can be part of predicate logic. Then, convince yourself that if it were true, it would be false, and if it were false, it would be true. This is indeed a contradiction.

Logicians have tried to escape this contradiction by outlawing self-references predicates. But here is a non-self-referencing form of the Liar's Paradox. First we form the predicate

$$P_{739}(x) = \text{The predicate } P_{740} \text{ is false.}$$

Then we form the predicate

$$P_{740}(x) = \text{The predicate } P_{739} \text{ is true.}$$

Now if P_{739} is true, then P_{740} is false, which means P_{739} is false. Thus P_{739} must be false. But then P_{740} is true so P_{739} is false. This is a contradiction.

One way to deal with this is to create hierarchies of predicates, and forbid a predicate from referring to a predicate from the same or higher level. But, we have no need to go into that.

3

Sets

3.1 Set Theory

The central primitive concepts in set theory are those of a *set* and set *membership*. We often denote a set by a letter, such as A, a, $\mathbf{a}$, $\mathbb{A}$, or $\mathbf{A}$. A set is simply a collection of things, and we call an element of such a collection a *member* of the set. We allow sets to be members of other sets. We write

$$a \in A \tag{3.1}$$

to mean that a is a member of set A, and

$$a \notin A \tag{3.2}$$

to mean that a is not a member of set A, or $\neg(a \in A)$, using the logical notation of the previous chapter. If $a \in A$, we also say that a is an *element* of A. The concept of set membership $\in$ is obviously primitive—we can interpret it clearly, but we do define it in terms of more elementary concepts.

We develop the axioms of set theory in section 3.15. According to one of these, the **Axiom of Extensionality**, we can always denote a set unambiguously by its elements, as for instance in

$$A = \{1, a, t, x\}, \tag{3.3}$$

meaning the set A consists of the number 1, and whatever the symbols a, t, and x represent.

By the Axiom of Extensionality, a set is completely determined by its members, and not how they are ordered. Thus the set A in (3.3) is the same as the set

$$\{a, x, 1, t\}$$

and even the same as the set

$$\{x, t, a, 1, 1, 1, t, a, t, x\}.$$

3.2 Properties and Predicates

We can represent a set in terms of the *properties* that are satisfied by the members of the set. Let $P(x)$ be shorthand for some property that may or may not be satisfied by a thing x. We call P a *predicate*. When $P(x)$ is true, we say "x has property P." For instance, suppose $P(x)$ means "x is a natural number divisible by 2." If we denote the natural numbers by $\mathbb{N} = \{0, 1, 2, \ldots\}$, the set A of natural numbers divisible by 2 is

$$A = \{x \in \mathbb{N} | P(x)\}. \tag{3.4}$$

This is probably the single most important notational device in mathematics, so you should make sure you understand it well: $\{--- | +++\}$ always means "the $---$ such that $+++$."

By the way, we will use the natural numbers as though we know what they are, for illustrative purposes. We define them later in terms of (what else?) sets.

We can write (3.4) in logical notation as

$$(\forall x \in \mathbb{N})(x \in A \leftrightarrow P(x)), \tag{3.5}$$

which reads "for all x in $\mathbb{N}$, x is in A if and only if x is divisible by 2." The upside-down A means "for all", and is called the *universal quantifier*—you will see it many, many times. The symbol $\leftrightarrow$ means "if and only if." By the way, there is another quantifier call the *existential quantifier*, written like backwards E ($\exists$). We can define either quantifier in terms of the other, using the concept of *negation* ($\neg$), which means "not": we have

$$(\forall x) P(x) \equiv \neg(\exists x)(\neg P(x)). \tag{3.6}$$

In words "P(x) is true for all x" means the same thing as "there does not exist an x for which $P(x)$ is false." We similarly have

$$(\exists x) P(x) \equiv \neg(\forall x)(\neg P(x)). \tag{3.7}$$

How is this expressed in words?

In general, if P is any predicate, we write the ensemble of things for which P is true as

$$\{x | P(x)\}, \tag{3.8}$$

and if we want to restrict the ensemble to things that belong to another ensemble S, we write

$$\{x \in S | P(x)\}. \tag{3.9}$$

We also say "$P(x)$" as a shorthand for "$P(x)$ is true." Thus we can read (3.9) as "the set of all $x \in S$ such that $P(x)$."

A second axiom of set theory is the **Axiom of Predication:** If A is a set and P is a predicate, then $\{x \in A | P(x)\}$ is also a set. This says we can freely construct subsets of a set corresponding to any determinate, expressible property $P(x)$. The Axiom of Predication (which is called infelicitously in the literature the "axiom of separation") allows us to carve out a piece of a set and we get a new set.

A third axiom of set theory is the **Power Set Axiom**, which says that if A is a set, then there is another set, we sometime write as $\mathcal{P}(A)$ and sometimes as 2^A, consisting of all the subsets of set A. For instance, if $A = \{a, b, c\}$ and a, b, and c are pairwise distinct (i.e., $a \neq b$, $b \neq c$, and $c \neq a$), then we have

$$2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{ab\}, \{ac\}, \{bc\}, \{abc\}\}. \tag{3.10}$$

Note that if we write $|A|$ to mean the number of elements in the set A, then we have $|2^A| = 2^{|A|}$. You will see later why we use this odd notation. The reason for the "pairwise distinct" qualification is that if $a = b = c$, then

$$\{a\} = \{b\} = \{c\} = \{a, b\} = \{a, c\} = \{b, c\} = \{a, b, c\}.$$

As we will see when we deal with Russell's Paradox, you cannot assume that the ensemble of things that satisfy an arbitrary predicate is a set. This is because the existence of such a set could lead to logical contradictions. However, we can use the term *class* to describe the ensemble of things that satisfy an arbitrary predicate. Indeed, we can formally *define* a class to be a predicate, so if we define the class $A = \{x | P(x)\}$, then $a \in A$ means neither more nor less than $P(a)$. This ploy may seem of questionable value, but note that if a is a class but not a set, then it does not make sense to write $a \in A$ no matter what A is, because set membership, $\in$, is only meaningful when what comes after the $\in$ is a set.

A class that is not a set is called a *proper class*. We can thus say a proper class C is a *subclass* of a proper class $\mathcal{C}$, meaning that each element of C is an element of $\mathcal{C}$, but not that it C is an element of $\mathcal{C}$. The elements of classes must themselves be sets. Russell's paradox, presented below, show the evil results of ignoring the distinction between a class and a set.

3.3 Operations on Sets

We say set A *equals* set B if they have the same members. Then, by the Axiom of Extensionality, two sets are equal if and only if they are the same set. For instance

$$\{1, 2, 3\} = \{2, 1, 3\} = \{1, 1, 2, 3\}.$$

If every member of set A is also a member of set B, we say A is a *subset* of B, and we write

$$A \subset B \qquad \text{or} \qquad A \subseteq B.$$

The first of these expressions says that A is a subset of B and $A \neq B$, while the second says that A is a subset of B but A may or may not equal B. For instance $\{x, t\} \subset \{x, t, 1\}$. For any set A, we then have $A \subseteq A$.

In formal mathematical notation, we define

$$A \subseteq B \equiv (\forall x \in A)(x \in B)$$
$$A \subsetneq B \equiv (\forall x \in A)(x \in B) \wedge (A \neq B)$$

In the second equation, the symbol $\wedge$ is logical notation for "and." Sometimes writers treat $\subset$ as meaning $\subseteq$ and others treat $\subset$ as meaning $\subsetneq$. When $A \subsetneq B$, we say A is a *proper subset* of B.

For any set A we have $\emptyset \subseteq A$, and if $A \neq \emptyset$, then $\emptyset \subsetneq A$. Can you see why? Hint: use (3.6) and show that there is no member of $\emptyset$ that is not a member of A.

Another commonly used notation is $A \backslash B$ or $A - B$, where A and B are sets, to mean the subset of A consisting of elements not in B. We call $A \backslash B$ the *difference* between A and B. Using logical notation,

$$A - B = A \backslash B = \{x | x \in A \wedge x \notin B\}. \tag{3.11}$$

We know that $A \backslash B$ is a set because it is the subset of A defined by the property $P(x) = x \notin B$.

The *union* sets A and B, which we write $A \cup B$, is the set of things that are members of either A or B. In mathematical language, we can write this as

$$A \cup B = \{x | x \in A \vee x \in B\}.$$

Here, the symbol $\vee$ means "or." For instance, $\{1, x, a\} \cup \{2, 7, x\} = \{1, x, a, 2, 7\}$.

For any set A, we have $A \cup \emptyset = A$. Do you see why?

The *intersection* of two sets A and B, which we write $A \cap B$, is the set of things that are members of both A and B. We can write this as

$$A \cap B = \{x | x \in A \wedge x \in B\}.$$

For instance, $\{1, x, a\} \cap \{2, 7, x\} = \{x\}$.

For any set A, we have $A \cap \emptyset = \emptyset$. Can you see why?

We say sets A and B are *disjoint* if they have no elements in common; i.e., if $A \cap B = \emptyset$ Can you see why?

For any two sets A and B, we have

$$A \cup B = (A \backslash B) \cup (A \cap B) \cup (B \backslash A), \tag{3.12}$$

and the three sets are mutually disjoint. This is illustrated in figure 3.1

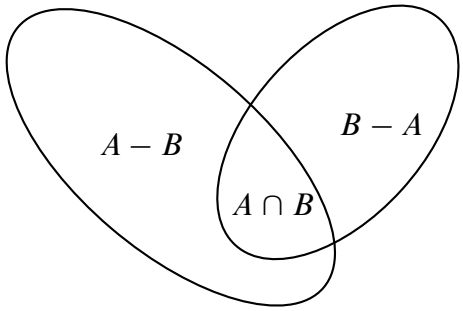

Figure 3.1. Set Differences, Intersections, and Unions

3.4 Russell's Paradox

Our treatment of set theory is perfectly intuitive, and it is hard to believe that it could ever get us into trouble. However, the famous philosopher Bertrand Russell showed that if you call any collection of things that can be characterized by a predicate a "set," and you assume any set can be a member of another set, you quickly arrive at a logical contradiction.

To see this, and to give the reader some practice in using the set notation, note that the ensemble of all sets is a class $\mathcal{S}$ represented by the predicate $P(x) = (x = x)$. Suppose the class of all sets were a set. Consider the property K such that $K(x)$ is true of a set x if and only if $x \notin x$. For instance, $K(\mathbb{N})$ is true because the set of natural numbers $\mathbb{N}$ is not itself a

natural number, and hence $\mathbb{N} \notin \mathbb{N}$. On the other hand, let $\mathcal{I}$ be the class of all sets with an infinite number of members (don't worry now about how exactly we define "infinite"; just use your intuition). Then clearly $\mathcal{I} \in \mathcal{I}$ because $\mathcal{I}$ has an infinite number of members. Hence $K(\mathcal{I})$ is false; i.e., $\mathcal{I}$ is a member of itself.

Now define a set $\mathcal{A}$ by

$$\mathcal{A} = \{x \in \mathcal{S} | K(x)\}.$$

i.e., $\mathcal{A}$ is the set of sets that are not members of themselves. Since $\mathcal{S}$ is a set by assumption, the Axiom of Predication implies that $\mathcal{A}$ is a set. Therefore either $\mathcal{A}$ is or is not a member of itself. If $\mathcal{A} \in \mathcal{A}$, then $K(\mathcal{A})$ is false, so $\mathcal{A} \notin \mathcal{A}$. Thus it must be the case that $\mathcal{A} \notin \mathcal{A}$. But then $K(\mathcal{A})$ is true, so $\mathcal{A} \in \mathcal{A}$. This is a contradiction, showing that our assumption that the ensemble of all sets, $\mathcal{S}$ is itself a set. We have proven that $\mathcal{S}$ is a proper class.

By the way, the method of prove used in the last paragraph is called *prove by contradiction* or *reductio ad absurdum*.

We say a mathematical system is *consistent* if it contains no contradictions. Many mathematicians and logicians spent a lot of time in the first few decades of the twentieth century in formulating a consistent set theory. They apparently did so successfully by outlawing huge things like "the set of all infinite sets," and always building large sets from smaller sets, such as the so-called *empty set*, written $\emptyset$, that has no elements. I say "apparently" because no one has ever found a contradiction in set theory using the Zermelo-Fraenkel axioms, which we discuss in section 3.15. On the other hand, according to a famous theorem of Gödel, if we could prove the consistency of set theory within set theory, then set theory would be *inconsistent* (figure that one out!). Moreover, since all of mathematics is based on set theory, there cannot be a mathematical theory that proves the consistency of set theory.

People love to say that mathematics is just tautological and expresses no real truth about the world. This is just bunk. The axioms of set theory, just like the axioms of logic that we develop later, were chosen because we expect them to be true. You might ask why mathematicians do not spend time empirically validating their axioms, if they might be false. The answer is that if an axiom is false, then some of the theorems it implies will be false, and when engineers and scientists use these theorems, they will get incorrect results. Thus, all of science is an empirical test of the axioms of set theory.

As we shall see, however, there are some sets that exist mathematically but are not instantiated in the real world. For instance, the natural numbers $\mathbb{N}$ are infinite in number, and there are only a finite number of particles in the Universe, so you can't play around with a physically instantiated copy of $\mathbb{N}$.

Before going on, you should reread the previous paragraphs and make sure you understand perfectly each and every expression. This will slow you down, but if you are used to reading normal English, you must understand that reading and understanding a page of math is often as time-consuming as reading and understanding twenty-five pages of English prose. This is not because math is harder than prose, but rather because mathematical expressions are compressed abbreviations of long and often complex English sentences.

3.5 Ordered Pairs

Sometimes we care not only about what members a set has, but also in what order they occur, and how many times each entry occurs. An *ordered pair* is a set with two elements, possibly the same, in which one is specified as the first of the two and the other is the second. For instance, the ordered pair (a, b) has first element a and second element b. By definition, we say $(a, b) = c$ exactly when c is an ordered pair, say $c = (d, e)$, and $a = d$ and $b = e$.

We could simply designate an ordered pair as a new fundamental concept along side the set and the member of relationship. However, there is an easy way to define an ordered pair in terms of sets. We define

$$(a, b) \equiv \{a, \{b\}\}. \tag{3.13}$$

You can check that this definition has the property that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Note that $\{a\} \neq \{a, \{a\}\}$. This is because the set $\{a\}$ has only one member, but the set $\{a, \{a\}\}$ has two members. Actually, we need a set theory axiom to show that no set can equal the set of which that set is the only member.

We can now define ordered triples as

$$(a_1, a_2, a_3) \equiv ((a_1, a_2), a_3), \tag{3.14}$$

and more generally, for $n > 3$

$$(a_1, \ldots, a_n) \equiv ((a_1, \ldots, a_{n-1}), a_n). \tag{3.15}$$

The notation $a_1, \ldots, a_n$ is very commonly used, and is a shorthand for the English expression "a_1 through a_n." For instance

$$(a_1, \ldots, a_7) = (a_1, a_2, a_3, a_4, a_5, a_6, a_7).$$

Another noteworthy property of the definition (3.15) is that it is *recursive*: we define the concept for low values of n (in our case, $n = 2$ and $n = 3$) and then for any greater n, we define the concept in terms of the definition for $n - 1$.

3.6 Mathematical Induction

The set $\mathbb{N}$ of natural numbers has one extremely important property. Let P be a predicate. Suppose $P(0)$ is true, and whenever $P(k)$ is true, you can prove $P(k + 1)$ is true. Then $P(k)$ is true for all $k \in \mathbb{N}$. Proving propositions about natural numbers in this manner is termed *mathematical induction*. More generally, if $P(k_0)$ is true for $k_0 \in \mathbb{N}$, and from $P(k)$ we can infer $P(k + 1)$, then $P(k)$ is true for all $k \geq k_0$.

As an exercise, we will use mathematical induction to prove that two ordered sets $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_r)$ are equal if and only if $k = r$, $k \geq 2$, and $a_i = b_i$ for $i = 1, \ldots, r$. First, suppose these three conditions hold. If $k = 2$, the conditions reduce to the definition of equality for ordered pairs, and hence the assertion is true for $k = 2$. Now suppose the assertion is true for any $k \geq 2$, and consider the ordered sets $(a_1, \ldots, a_{k+1})$ and $(b_1, \ldots, b_{k+1})$. We can rewrite these sets, by definition, as $((a_1, \ldots, a_k), a_{k+1})$ and $((b_1, \ldots, b_k), b_{k+1})$. Because of the induction assumption, we have $(a_1, \ldots, a_k) = (b_1, \ldots, b_k)$ and $a_{k+1} = b_{k+1}$, and hence by the definition of equality of ordered pairs, we conclude that $(a_1, \ldots, a_{k+1}) = (b_1, \ldots, b_{k+1})$. Therefore the assertion is true for all $k \geq 2$ by mathematical induction.

I invite the reader to prove the other direction. It goes something like this. First, suppose $(a_1, \ldots, a_k) = (b_1, \ldots, b_r)$ and $k \neq r$. Then there is a smallest k for which this is true, and $k > 2$ because we know that an ordered pair can never be equal to an ordered set of length greater than 2. But then by definition, $((a_1, \ldots, a_{k-1}), a_k) = ((b_1, \ldots, b_{r-1}), b_r)$. Because the first element of each of these ordered paris must be equal, we must have $(a_1, \ldots, a_{k-1}) = (b_1, \ldots, b_{r-1})$, and by the induction assumption, we conclude that $k - 1 = r - 1$, so $k = r$. Thus our assumption that $k \neq r$ is false, which proves the assertion.

3.7 Set Products

The *product* of two sets A and B, written $A \times B$, is defined by

$$A \times B \equiv \{(a,b)|a \in A \text{ and } b \in B\}. \tag{3.16}$$

For instance,

$$\{1,3\} \times \{a,c\} = \{(1,a),(1,c),(3,a),(3,c)\}.$$

A more sophisticated example is

$$\mathbb{N} \times \mathbb{N} = \{(m,n)|m,n \in \mathbb{N}\}.$$

Note that we write $m,n \in \mathbb{N}$ as a shorthand for "$m \in \mathbb{N}$ and $n \in \mathbb{N}$."

We can extend this notation to the product of n sets, as in $A_1 \times \ldots \times A_n$, which has typical element $(a_1,\ldots,a_n)$. We also write $A^n = A \times \ldots \times A$, with the convention that $A^1 = A$.

3.8 Relations and Functions

If A and B are sets, a binary *relation* R on $A \times B$ is simply a subset of $A \times B$. If $(a,b) \in R$ we write $R(a,b)$, or we say "R(a,b) is true." We also write $R(a,b)$ as aRb when convenient. For instance, suppose R is the binary relation on the real numbers such that $(a,b) \in R$, or aRb is true, exactly when $a \in \mathbf{R}$ is less than $b \in \mathbf{R}$. Of course, we can replace aRb by the convention notation $a < b$, as defining R had the sole purpose of convincing you that "$<$" really is a subset of $R \times R$. In set theory notation,

$$<= \{(a,b) \in \mathbf{R} \times \mathbf{R}|a \text{ is less than } b\}.$$

Other binary relations on the real numbers are $\leq$,$>$, and $\geq$. By simple analogy, an n-ary on $A_1 \ldots A_n$ $n \in \mathbb{N}$ and $n > 2$ is just a subset of $A_1 \ldots A_n$. An example of a trinary relation is

$$a = b \bmod c \quad = \quad \{(a,b,c)|a,b,c \in \mathbb{Z} \wedge (\exists d \in \mathbb{Z})(a-b = cd)\}.$$

In words, $a = b \bmod c$ if $a - b$ is divisible by c.

A *function*, or *mapping*, or *map* from set A to set B is a binary relation f on $A \times B$ such that for all $a \in A$ there is exactly one $b \in B$ such that afb. We usually write afb as $f(a) = b$, so $f(a)$ is the unique value b

for which afb. We think of a function as a *mapping* that takes members of A into unique members of B. If $f(a) = b$, we say b is the *image* of a under f. The *domain* Dom(f) of a function f is the set A, and the *range* Range(f) of f is the set of $b \in B$ such that $b = f(a)$ for some $a \in A$. We also write the range of f as $f(A)$, and we call $f(A)$ the *image* of A under the mapping f.

We write a function f with domain A and range included in B as $f:A \rightarrow B$. In this case $f(A) \subseteq B$ but the set inclusion need not be a set equality.

We can extend the concept of a function to n dimensions for $n > 2$, writing $f : A_1 \times \ldots \times A_n \rightarrow B$ and $f(a_1, \ldots, a_n) = b$ for a typical value of f. Again, we require b to be unique. Indeed, you can check that a function is just an $(n + 1)$-ary relation R in which, for any n-tuple $a_1, \ldots, a_n$, there is a unique a_{n+1} such that $R(a_1, \ldots, a_n, a_{n+1})$. We then write $R(a_1, \ldots, a_n, a_{n+1})$ as $f(a_1, \ldots, a_n) = a_{n+1}$.

Note that in the previous paragraph we used without definition some obvious generalizations of English usage. Thus an n-tuple is the generalization of double and triple to an ordered set of size n, and n-ary is a generation of binary to ordered n-tuples.

3.9 Properties of Relations

We say a binary relation R with domain D is *reflexive* if aRa for any $a \in D$, and R is *irreflexive* if $\neg aRa$ for all $a \in D$. For instance, $=$ is reflexive but $<$ is irreflexive. Note that $\leq$ is neither reflexive nor irreflexive.

We say R is *symmetric* if $(\forall a, b \in D)(aRb \rightarrow bRa)$, and R is *anti-symmetric* if for all $a, b \in D$, aRb and bRa imply $a = b$. Thus $=$ is symmetric but $\leq$ is anti-symmetric. Finally, we say that R is *transitive* if $(\forall a, b, c \in D)(aRb \wedge bRc \rightarrow aRc)$. Thus, in arithmetic, '$=$', '$<$', '$>$', '$\leq$', '$>$', and $\geq$' are all transitive. An example of a binary relation that is not transitive is '$\in$', because the fact that $a \in A$ and $A \in S$ does not imply $a \in S$. For instance $1 \in \{1, 2\}$ and $\{1, 2\} \in \{2, \{1, 2\}\}$, but $1 \notin \{2, \{1, 2\}\}$.

A relation R that is reflexive, symmetric, and transitive is called an *equivalence relation*. In arithmetic, $=$ is an equivalence relation, while $<$, $>$, $\leq$, '$>$', and $\geq$' are not equivalence relations.

If R is an equivalence relation on a set D, then there is a subset $A \subseteq D$ and sets $\{D_a | a \in A\}$, such that

$$(\forall a, b \in A)(\forall c \in D_a)(\forall d \in D_b)((aRc) \wedge ((a \neq b) \rightarrow \neg aRd)).$$

This is an example of how a mathematical statement can look really complicated yet be really simple. This says that we can write D as the union of mutually disjoint sets $D_a, D_b, \ldots$ such that cRd for any two elements of the same set D_a, and $\neg cRd$ if $c \in D_a$ and $d \in D_b$ where $a \neq b$. For instance, suppose we say two plane geometric figures are *similar* if one can be shrunk uniformly until it is coincident with the other. Then similarity is an equivalence relation, and all plane geometric figures can be partitioned into mutually disjoint sets of similar figures. We call each such subset a *cell* of the partition, or an *equivalence class* of the similarity relation.

Another example of an equivalence relation, this time on the natural numbers $\mathbb{N}$, is $a \equiv b \mod k$, which means that the remainder of a divided by k equals the remainder of b divided by k. Thus, for instance $23 \equiv 11 \mod 4$. In this case $\mathbb{N}$ is partitioned into four equivalence classes, $\{0, 4, 8, 12, \ldots\}$, $\{1, 5, 9, 13, \ldots\}$, $\{2, 6, 10, 14 \ldots\}$, and $\{3, 7, 11, 15, \ldots\}$. The relation $a \equiv b \mod c$ is a trinary relation.

3.10 Injections, Surjections, and Bijections

If $f : A \to B$ is a function and $\text{Range}(f) = B$, we say f is *onto* or *surjective*, and we call f a *surjection*. Sometimes, for a subset A_s of A, we write $f(A_s)$ when we mean $\{b \in B | (\exists a \in A_s)(b = f(a)\}$. This expression is another example of how a simple idea looks complex when written in rigorous mathematical form, but becomes simple again once you decode it. This says that $f(A_s)$ is the set of all b such at $f(a) = b$ for some $a \in A_s$. Note that $f(A) = \text{Range}(f)$.

As an exercise, show that if $f : A \to B$ is a function, then the function $g : A \to f(A)$ given by $g(a) = f(a)$ for all $a \in A$, is a surjection.

If f is a function and $f(a) = f(b)$ implies $a = b$, we say f is *one-to-one*, or *injective*, and we call f a *injection*. We say f is *bijective*, or is a *bijection* if f is both one-to-one and onto.

If $f : A \to B$ is injective, there is another function: $\text{Range}(f) \to A$ such that $g(b) = a$ if and only if $f(a) = b$. We call g the *inverse* of f, and we write $g = f^{-1}$, so $g(f(a)) = f^{-1}(f(a)) = a$. As an exercise show that f^{-1} cannot be uniquely defined unless f is injective. For instance, suppose $f : \mathbb{Z} \to \mathbb{Z}$ is given by $f(k) = k^2$, where BbZ is the set of integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. In this case, for any $k \in \mathbb{Z}$, $f(k) = f(-k)$, so for any square number k, there are two equally valid candidates for $f^{-1}(k)$.

Note that if r is a number, we write $r^{-1} = 1/r$, treating the -1 as a power, as you learned in elementary algebra. However, if f is a function, the -1 exponent in f^{-1} means something completely different, namely the inverse function to f. If f is a function whose range is a set of non-zero numbers, we can define $(f)^{-1}$ as the function such that $(f)^{-1}(a) = 1/f(a)$, but f^{-1} and $(f)^{-1}$ are usually completely different functions (when, dear reader, are the two in fact the same function?).

Note that if $f : A \to B$ is a function then f^{-1} is surjective by definition. Is it one-to-one? Well, if $f^{-1}(a) = f^{-1}(b)$, then $f(f^{-1}(a)) = f(f^{-1}(b))$, so $a = b$; i.e., f^{-1} is injective, and since it is also surjective, it is a bijection. You can easily show that if f is an injection, then $f : A \to \text{Range}(f)$ is bijective.

3.11 Counting and Cardinality

If two sets have equal size, we say the have the same *cardinality*. But, how do we know if two sets have equal size? Mathematicians have come to see that the most fruitful and consistent definition is that two sets are of equal size if there exists a bijection between them. We write the cardinality of set A as $\mathbf{c}(A)$, and if A and B have the same cardinality, we write $\mathbf{c}(A) = \mathbf{c}(B)$, or equivalently $A \sim B$. The most important property of $\sim$ is that it is an equivalence relation on sets. First, for any set A, we have $A \sim A$ because the identity function i from A to A such that $(\forall a \in A)(i(a) = a)$ is a bijection between A and itself. Thus $\sim$ is reflexive. Moreover if f is a bijection from A to B, then f^{-1} is a bijection from B to A. Thus $(A \sim B) \leftrightarrow (B \sim A)$, so $\sim$ is symmetric. Finally if f is a bijection from A to B and f is a bijection from B to C, then the *composite function* $g \circ f : A \to C$, where $g \circ f(a) = g(f(a))$, is a bijection from A to C. Thus $\sim$ is transitive. Like every other equivalence relation, $\sim$ defines a partition of the class of sets into sub-classes such that for any two members s and t of the equivalence class, $s \sim t$, and if s and t come from difference equivalence classes $\neg(s \sim t)$. We call these equivalence classes *cardinal numbers*.

If there is a one-to-one map from A to B, we write $\mathbf{c}(A) \leq \mathbf{c}(B)$, or equivalently, $A \preceq B$, or again equivalently, $\mathbf{c}(B) \geq \mathbf{c}(A)$, or $B \succeq A$. The binary relation $\preceq$ is clearly reflexive and transitive, but it is not symmetric; e.g., $1 \leq 2$ but $\neg(2 \leq 1)$.

One property we would expect $\preceq$ to satisfy is that $A \preceq B$ and $B \preceq A$, then $A \sim B$. This is of course true for finite sets, but in general it is not obvious. For instance, the positive *rational numbers* $\mathbb{Q}^+$ are defined as follows:

$$\mathbb{Q}^+ \equiv \left\{ \frac{m}{n} \,\middle|\, m, n \in \mathbb{N}, n \neq 0 \right\}. \tag{3.17}$$

We also define a relation $=$ on $\mathbb{Q}^+$ by saying that $m/n = r/s$ where $m/n, r/s \in \mathbb{Q}^+$ if and only if $ms = rn$. We consider all members of the same equivalence classes with respect to $=$ to be the same rational number. Thus, we say $3/2 = 6/4 = 54/36$. It is obvious that $\mathbb{N} \preceq \mathbb{Q}$ because we have the injection f that takes natural number k into positive rational number $k/1$. We can also see that $\mathbb{Q}^+ \preceq \mathbb{N}$. Let $q \in \mathbb{Q}^+$ and write $q = m/n$ where $m + n$ is as small as possible. Now let $g(q) = 2^m 3^n$. Then g is a mapping from $\mathbb{Q}^+$ to $\mathbb{N}$, and it is an injection, because if $2^a 3^b = 2^c 3^d$ where a, b, c, d are any integers, then we must have $a = c$ and $b = d$. Thus we have both $\mathbb{N} \preceq \mathbb{Q}^+$ and $\mathbb{Q}^+ \preceq \mathbb{N}$.

However $\mathbb{N} \sim \mathbb{Q}^+$ only if there is a bijection between $\mathbb{Z}$ and $\mathbb{Q}$. Injections in both directions are not enough. In fact, there is one easy bijection between $\mathbb{Q}^+$ and $\mathbb{N}$. Here is a list of the elements of $\mathbb{Q}^+$ as a sequence:

$$0, 1, 2, 3, 1/2, 4, 1/3, 5, 3/2, 2/3, 1/4,$$
$$6, 1/5, 7, 5/2, 4/3, 3/4, 2/5, 1/6, \ldots$$

We generate this sequence by listing all the fractions m/n such that $m+n = k$ for some k, starting with $k = 0$, and drop any fraction that has already appeared in the sequence (thus 2 is included, but then 1/1 is dropped; 4 is included but 3/1 is dropped). Now for any $q \in \mathbb{Q}^+$, let $f(q)$ be the position of q in the above sequence. Thus $\mathbb{Q} \sim \mathbb{Z} \sim \mathbb{N}$.

3.12 The Cantor-Bernstein Theorem

The amazing thing is that the for any two sets A and B, if $A \preceq B$ and $B \preceq A$ then $A \sim B$. This is called the **The Cantor-Bernstein Theorem**. The proof of this theorem is not complex or sophisticated, but it is a bit tedious. It will be a challenge for the reader to go through the proof until it is transparent.

To prove the Cantor-Bernstein Theorem, suppose there is a one-to-one mapping $f : A \to B$ and a one-to-one mapping $g : B \to A$. How can we construct therefrom a bijection $h : A \to B$?

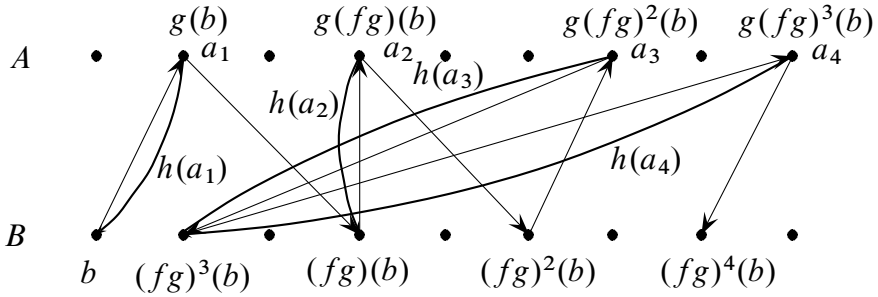

Figure 3.2. The Cantor-Bernstein Theorem

Because f is an injection, $f:A\to f(A)$ is a bijection. Similarly, $g:B\to g(B)$ is a bijection. If $B = f(A)$ we are done, so suppose $b \in B - f(A)$. Then for all $k \in \mathbb{N}$, if $a = (g \circ f)^k g(b)$, we define $h(a) = b'$, where $g(b') = a$. In other words, we consider all sequences in A of the form

$$s(b) = \{g(b), gfg(b), (gf)^2 g(b), (gf)^3 g(b) \ldots\}$$

and we define

$$h(g(b)) = b, \quad h(gfg(b)) = fg(b), \quad h((gf)^2 g(b)) = (fg)^2(b), \ldots$$

Note that $f \circ g(b)$ means the same thing as $fg(b)$, $f \circ g \circ f(a)$ means the same thing as $fgf(a)$, and so on. This is illustrated in figure 3.2. Clearly, this process will iterate an infinite number of times, or $h(a)$ points back to some previous point in the sequence, and we can do no more with this sequence.

We repeat this construction for all $b \in B - f(A)$. We call an $a \in A$ *uncovered* if $h(a)$ is undefined, and we define $h(a) = f(a)$ if a is uncovered. Thus h is a relation with domain A. We must show that (a) h is a function; (b) h is an injection; and (c) h is a surjection.

To see that h is a function, we must show that $h(a)$ is defined exactly once for each $a \in A$. Because both f and g are injections, $s(b)$ and $s(b')$ are disjoint (i.e., have no members in common) if $b, b' \in B - f(A)$ and $b \neq b'$. To see this, note that $b \neq b'$ implies $g(b) \neq g(b')$. Now $g(b)$ cannot occur anywhere in $s(b')$ because all members of $s(b')$ except the first are in the image of f while by definition $g(b)$ is not. Now we use mathematical induction and *reductio ad absurdum*. Suppose we have proved

that $(gf)^k g(b)$ is not in $s(b')$, but $(gf)^{k+1}g(b)$ is in $s(b')$. We cannot have $(gf)^{k+1}g(b) = g(b')$ because b' is not in the image of f, whereas $(gf)^{k+1}g(b)$ clearly is. But if $(gf)^{k+1}g(b) = (gf)^j g(b')$ for $j > 0$, then since f and g are injections, we have $(gf)^{k-j+1}g(b) = g(b')$, which we have already shown is not the case. Because the $\{s(b)|b \in B - f(A)\}$ are disjoint, and $h(a)$ is defined as $f(a)$ if and only if $h(a)$ is not defined by one of the $s(b)$, h is a function.

Now we want to show that the function h is injective. Suppose that both a_1 and a_2 are uncovered and $h(a_1) = h(a_2)$. If $h(a_1) = f(a_1)$ and $h(a_2) = f(a_2)$, then $a_1 = a_2$, because f is one-to-one. If both a_1 and a_2 are covered, let $h(a_1) = b_1$ where $g(b_1) = a_1$ and $h(a_2) = b_2$ where $g(b_2) = a_2$. Then $a_1 = a_2$ because g is an injection. Finally, suppose a_1 is covered and a_2 is uncovered. Then $a_1 = gh(a_1)$ and $h(a_2) = f(a_2)$. We can write $a_1 = (gf)^n g(b_0)$ with $n \geq 0$ and $b_0 \in B - f(A)$. Then we have $(gf)^n g(b_0) = a_1 = gh(a_1) - gh(a_2) = gf(a_2)$. If $n = 0$, $b_0 = hf(a_2)$, so $b_0 \in f(A)$, which is a contradiction. Thus $n > 0$, and since gf is an injection, we can cancel one gf from both sides of $(gf)^n g(b_0) = gf(a_2)$, getting $(gf)^{n-1}g(b_0) = a_2$. But then a_2 is covered, counter to our assumption. This proves that h is injective.

To see that h is surjective, let $b \in B$. If $b \notin f(A)$, then $s(b)$ is a sequence whose first element is b with $g(b) = a \in A$, so $h(a) = b$. If $b \in f(A)$ but b is a member of some sequence $g(b')$, then $b = (gf)^j g(b')$ and if $a = g(b)$, then $h(a) = b$. If b is not a member of a sequence and $g(b) = a$, then a will not be covered, since g is injective. Thus $f(a) = b$. This proves h is a bijection.

It is always good to go through an example of a rather complicated algorithm such as the above. So let $A = \{2, 4, 6, 8, 10, \ldots\}$ and let $B = \{3, 6, 9, 12, 15, \ldots\}$ and the injections $f(k) = 3k$ from A to B and $g(k) = 2k$ from B to A. Of course, in this case there is an obvious bijection of A onto B, where $h(2k) = 3k$. However, this does not use f and g, and depends on the special nature of A and B. We will construct the bijection h using only the fact that they are injections. We do not have to be able to order A or B, nor need we know if they are finite or infinite. First, we have

$$B - f(A) = \{3, 9, 15, 21, 27, \ldots\} = \{3(2k + 1)|k \in \mathbb{N}\}.$$

Note that $f(A) = \text{Range}(f)$. You should make sure you understand clearly why the two sets are equal—substitute values 0,1,2, etc. for k in the second

set and compare the results with $\{3, 9, 15, 21, 27 \ldots\}$. *Never* just take the writer's word for things like this.

The elements of A of the form $(g \circ f)^k g(b)$ where $b \in B - f(A)$ are then

$$\begin{aligned} A^* &= \{(g \circ f)^j g(3(1+2k)) | j, k \in \mathbb{N}\} \\ &= \{2 \times 6^j \times 3(1+2k) | j, k \in \mathbb{N}\} \\ &= \{6^{j+1}(1+2k) | j, k \in \mathbb{N}\} \end{aligned}$$

For $a \in A^*$, we let $h(a) = a/2$, and for $a \notin A^*$, we let $h(a) = 3a$.

You can check that

$$A^* = \{6, 18, 30, 36, 42, 54, 66, 78, 90, 102, \ldots\}.$$

so

$$\begin{aligned} h(A) = \{&6, 12, 3, 24, 30, 36, 42, 48, 9, 60, 66, 72, 78, 84, 15, \\ &96, 102, 18, 114, \ 120, 21, 132, 138, 144, 150, \ldots\}. \end{aligned}$$

If you sort this set into ascending order, you will see that (a) there are no repeats, so h is injective, and (b) the range is B (actually, this is true only up to $b = 84$; you must extend the list to include $b = 90$, which is the image of $a = 180$ under h, because $180 = 6^2(1 + 2 \times 2 \in A^*)$.

3.13 Inequality in Cardinal Numbers

We say, naturally enough, that set A is smaller than set B, which we write $A \prec B$, if there is an injection f from A to B, but there is no bijection between A and B. From the Cantor-Bernstein Theorem, this means $A \prec B$ if and only if there is an injection of A into B, but there is no injection of B into A.

If S is a set and R is a binary relation on S we say R is *anti-symmetric* if, for all $x, y \in S$ with $x \neq y$ either xRy or yRx, but not both, are true. We say R is an *ordering* of S if R is anti-symmetric and transitive. We say set S is *well-ordered* if there is some ordering R on S such that every subset A of S has a smallest element. Note that this makes sense because such a smallest element must be unique, by the anti-symmetry property. For example '$<$' is an ordering on $\mathbb{N}$. By the way, we say a relation R is *trichotomous* if for all a, b, exactly one of aRb, bRa, or $a = b$ holds. Thus $\leq$ is anti-symmetric, but $<$ is trichotomous.

Let us write, for convenience, $\mathbb{N}_n = \{1, 2, \ldots, n\}$, the set of positive natural numbers less than or equal to n. Recall the we could also write $\mathbb{N}_n = \{k \in \mathbb{N} | 1 \leq k \leq n\}$. It should be clear that if $\mathbb{N}_n \sim \mathbb{N}_m$, then $m = n$. Thus, it is not unreasonable to identify the number of elements of a set with its cardinality when this makes sense.

We say a set A is *finite* if there is a surjective function $f : \mathbb{N}_n \to A$ for some natural number n, or equivalently, if there is an injective function $f : A \to \mathbb{N}_n$. We also want the empty set to be finite, so we add to the definition that $\emptyset$ is finite.

We say a set is *infinite* if it is not finite. You are invited to show that if set A has an infinite subset, then A is itself infinite. Also, show that $\mathbb{N}$ and $\mathbb{Z}$ are infinite. We say that a set is *countable* if it is either finite or has the same cardinality as $\mathbb{N}$. We write the cardinality of $\mathbb{N}$ as $\mathbf{c}(\mathbb{N}) = \aleph_0$.

3.14 Power Sets

The set of natural numbers, $\mathbb{N}$, is the "smallest" infinite set in the sense that (a) every subset of $\mathbb{N}$ is either finite or has the same cardinality as $\mathbb{N}$, which is $\aleph_0$. The great mathematician Georg Cantor showed that $\mathcal{P}(\mathbb{N})$, the power set of the natural numbers, has a greater cardinality than $\aleph_0$. Indeed, he showed that for any set A, $\mathbf{c}(A) < \mathbf{c}(\mathcal{P}(A))$.

To see this note that the function f that takes $a \in A$ into $\{a\} \in \mathcal{P}(A)$ is one-to-one, so $\mathbf{c}(A) \leq \mathbf{c}(\mathcal{P}(A))$. Suppose g is a function that takes each $S \in \mathcal{P}(A)$ into an element $g(S) \in A$, and assume g is one-to-one and onto. We will show that a contradiction flows from this assumption. For each $S \in \mathcal{P}(A)$, either $g(S) \in S$ or $g(S) \notin S$. Let $T = \{a \in A | a \notin g^{-1}(a)\}$, where $g^{-1}(a)$ is defined to be the (unique) member $S \in \mathcal{P}(A)$ such that $g(S) = a$. Then $T \subseteq A$, so $T \in \mathcal{P}(A)$. If $g(T) \in T$, then by definition $g(T) \notin T$. Thus $g(T) \notin T$. But then, by construction, $g(T) \in T$. This contradiction shows that g is not one-to-one onto, which proves the assertion.

3.15 The Foundations of Mathematics

In this section I want to present the so-called Zermelo-Fraenkel axioms of set theory. We have used most of them implicitly or explicitly already. You should treat this both as an exercise in reading and understanding the notation and concepts developed in this chapter. Also, substantively, perhaps for the first time in your life you will have some idea what sorts of assumptions underlie the world of mathematics. I won't prove any theorems, although

I will indicate what can be proved with these axioms. I am following the exposition by Mileti (2007).

Axiom of Existence: There exists a set.

You might fairly wonder exactly what this means, since the concept of "existence" is a deep philosophical issue. In fact, the Axiom of Existence means that the proposition $(\exists x)(x = x)$ is true for at least one thing, x.

Axiom of Extensionality: Two sets with the same members are the same.

Axiom of Predication: If A is a set, then so is $\{x \in A | P(x)\}$ for any predicate $P(x)$.

Now, it is a deep issue as to exactly what a predicate such as $P(x)$ really is. We will treat a predicate as a string of symbols that become meaningful in some language, and such that for each x, the string of symbols has the value $\top$ ("true") or $\bot$ ("false");

Note that these three axioms imply that there is a unique set with no elements, $\emptyset$, which we have called the *empty set*. To see this, let A be any set, the existence of which is guaranteed by the Axiom of Existence. Now let $P(x)$ mean $x \neq x$. The ensemble $B = \{a \in A | P(x)\}$ is a set by the Axiom of Predication. But B has no elements, so $B = \emptyset$. The empty set is unique by the Axiom of Extensionality.

Axiom of Parametrized Predication: If A is a set and $P(x, y)$ is a predicate such that for every $x \in A$ there is a unique set y_x such that $P(x, y)$ holds, then $B = \{y_x | x \in A\}$ is a set.

This is a good place to mention that we often use subscripts and superscripts to form new symbols. The symbol y_x is a good example. This can cause confusion, for instance if we write something like a^2, which could either mean $a \times a$ or the symbol $a - super - 2$. You have to figure out the correct meaning by context. For instance, if it doesn't mean anything to multiply a by itself, then clearly the second interpretation is correct.

The Axiom of Parametrized Predication is generally called the Axiom of Collection in the literature. I don't find this name very informative. Note that if the set A is finite, the set B whose existence is guaranteed by the Axiom of Parametrized Predication actually does not need the axiom. The Axiom of Union (see below) is enough in this case. Can you see why?

There is one especially important case where the Axiom of Parametrized Predication is used—one that is especially confusing to beginners. Suppose the predicate $P(x, y)$ in the axiom is $y = C$ for some set C, the same for all y. Then the set B consists of a copy of C for each $y \in A$. We write this as C^A. Note that a typical member of C^A consists of a member of C

for each $x \in A$. We can write this member of C^A as $f(x) = y$, where $f : A \to C$; i.e., members of C^A are precisely functions from A to C. Very often in the literature you will encounter something like "Let $f \in C^A$" rather than "Let $f : A \to C$." The two statements mean exactly the same thing.

Now you should understand why we expressed the power set of a set A not only as $\mathcal{P}(A)$, but also as 2^A. This is because if we think of the number 2 as the set consisting of the numbers zero and one (i.e., 2={0,1}), as we shall do in the next chapter, then a member of 2^A is just a function $f : A \to \{0, 1\}$, which we can identify with the subset of A where $f(x) = 0$. Clearly, there is a one-to-one corresponding between elements of 2^A and the functions from A whose values are zero and 1, so we can think of them as the same thing.

Axiom of Pairing: If x and y are sets, then so is $\{x, y\}$.

Thus, for instance, $\{\emptyset, \emptyset\}$ is a set, and by the Axiom of Extensionality, this is just $\{\emptyset\}$. Note that this set is not the same as $\emptyset$ because is isn't empty—it has the member $\emptyset$!

By the same reasoning, for any set A there is a new set $\{A\}$ whose only member is A. We thus have a sequence, for instance, of pairwise distinct sets

$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \ldots$$

Axiom of Union: If x and y are sets, then so is $x \cup y$.

Using this axiom, we can form new sets like $\{\emptyset, \{\emptyset\}\}$, which is the first example we have of a set with two elements. Later, we will see that the entire number system used in mathematics can be generated from the empty set $\emptyset$, using the axioms of set theory. This is truly building something out of nothing.

Power Set Axiom If A is a set, then there is a set $\mathcal{P}(A)$, called the *power set* of A, such that ever subset of A is an element of $\mathcal{P}(A)$.

While every element of $\mathcal{P}(A)$ is a definite subset of A, this does not mean that we can identify every subset using the Axiom of Predication. For instance, if a language has a finite number of primitive symbols (its 'alphabet'), then all the meaningful predicates in the language can be arranged in alphabetical order, and hence the meaningful predicates have the same cardinality as $\mathbb{N}$. But $\mathcal{P}(\mathbb{N})$ is larger than $\mathbb{N}$ (i.e., there is no injection of $\mathcal{P}(\mathbb{N})$ into $\mathbb{N}$, as we saw above), so we cannot specify most of the subsets of $\mathcal{P}(\mathbb{N})$ by means of predication.

Axiom of Infinity: For any set x define the *successor* $S(x)$ of x to be $S(x) = x \cup \{x\} = \{x, \{x\}\}$. Then there is a set A with $\emptyset \in A$ and for all $x \in A$, $S(x) \in A$. This set is infinite because one can prove that x can never equal $S(S(S \ldots S(x))$ for any number of repetitions of the successor function.

Axiom of Foundation: Every set A has a member x such that no member of x is a member of A. This axiom, along with the others, implies that there is no infinitely descending sequence of the form $\ldots \in x \in y \in z \in A$.

There are a few more axioms that are usually assumed, including the famous **Axiom of Choice** and the **Continuum Hypothesis**, but we will not go into these interesting but rather abstruse issues.

4

Numbers

4.1 The Natural Numbers

We have used the *natural numbers* $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ freely in examples, but not in formal definitions. We are now in a position to define the natural numbers in terms of sets. We call the result the *ordinal numbers* because they will be totally ordered by the usual notion of $<$. The empty set $\emptyset = \{\}$ is the set with no elements. For instance, the set of married bachelors is $\emptyset$. Let us define the symbol 0 (zero) to be $\emptyset$. Then if n is any number, define $n + 1$ as the set consisting of all numbers from 0 to n. Thus we have

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\}, \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \\ 3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\ 4 &= \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \end{aligned}$$

and so on.

4.2 Representing Numbers

As we will see, the above definition of a number is very easy to work with for theoretical purposes, but it would be a horror if we had to use it in practice. For instance, you can check that the number 25 would have $2^{24} =$ 16,777,216 copies of $\emptyset$ in its representation. The Romans moved a bit ahead of this by defining special symbols for 5, 10, 50, 100, 500, and 1000, but doing arithmetic with Roman numerals is extremely difficult.

The major breakthrough in representing numbers in a way that makes arithmetic easy was invented in India around 500 BP, and included a zero and positional notation with base 10. The symbols used today are 0 1 2 3 4 5 6 7 8 9, and a number written as $d_1 d_2 d_3$, for instance, is really $100 \cdot d_1 + 10 \cdot d_2 + d_3$. This number system is often termed *arabic*, and the

numerals 0, . . . , 9 are called *arabic numerals*. There is nothing sacrosanct about base 10, however. In computer science, base 2 ("binary") and base 16 ("hexidecimal") are commonly used. The symbols in base 2 are 0 1, and in base 16, 0 1 2 3 4 5 6 7 8 9 a b c d e f. So, for instance in base 16, the number abcd represents the decimal number 43,981 in decimal notation. This number in binary notation is 1010101111001101.

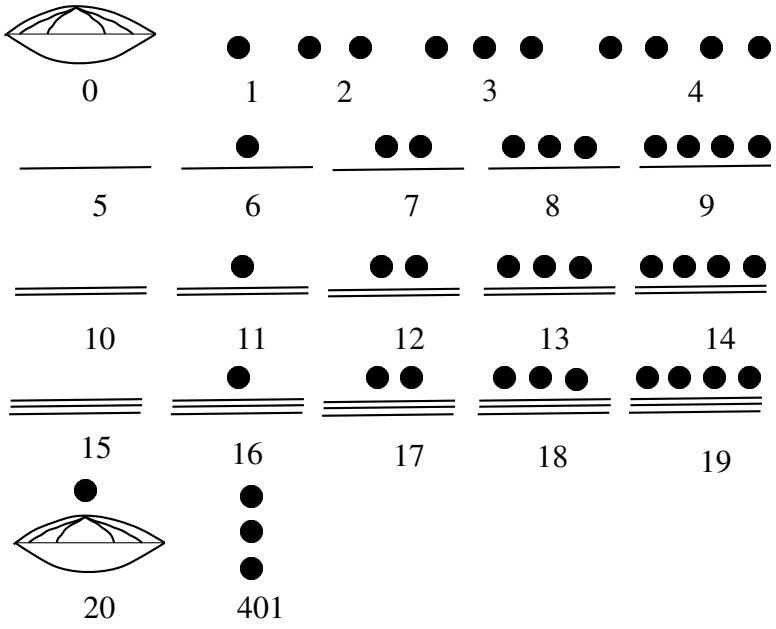

Figure 4.1. The Mayan Number System

Even more exotic was the ancient Mayan number system, which was fully modern in having both a number zero and a base-20 set of numeral symbols, as shown in figure 4.1. After the 20 symbols, the figure shows the number 20, which is 10 in the Mayan system, and the number 421, which is 111. The Mayans, as you can see, stack the composite numbers vertically rather than horizontally, as we do.

4.3 The Natural Numbers as an Ordered Commutative Semigroup

The ingenious thing about our definition of natural numbers is that we can define all arithmetical operations directly in terms of set theory. We first

define a total order on $\mathbb{N}$. A *total order* is a relation, which we will write as $\leq$, that has the following properties for all $n, m, r \in \mathbb{N}$:

if $a \leq b$ and $b \leq c$, then $a \leq c$	transitive
if $a \leq b$ and $b \leq a$, then $a = b$	antisymmetric
either $a \leq b$ or $b \leq a$	total.

Note that if $\leq$ is a total order and we define $<$ by $a < b$ if $a \leq b$ but $a \neq b$, then $<$ satisfies

if $a < b$ and $b < c$, then $a < c$	transitive
if $a < b$ implies $\neg(b < a)$,	asymmetric
either $a < b$ or $a = b$ or $b < a$	total.

In practice, we can think of either $\leq$ or $<$ as a total order, as either one is easily defined in terms of the other.

We can define natural number m to be *less than* ($<$) natural number n if $m \subset n$, or equivalently, if $m \in n$. With this definition, $0 < 1 < 2 < 3 \ldots$. Also $<$ is *transitive* because $m \subset n$ and $n \subset r$ implies $m \subset r$ in set theory. Moreover, $m < n$ implies $\neg(n < m)$. This is because if m is a proper subset of n, then n has an element that is not in m, so n cannot be a subset of m. Thus $<$ is asymmetric.

We can also show that for any two natural numbers m and n, either $m < n$, $m = n$ or $m > n$, so $<$ is total. To see this suppose there are two unequal numbers, neither of which is smaller than the other. Then there must be a smallest number m for which n exists with $n \neq m$ and not $m < n$ and not $n < m$. Let n be the smallest number with this property. Then either $m = n - 1$ or $m < n - 1$ or $m > n - 1$. But we cannot have $m = n - 1$ because then $m \in n$, so $m < n$. We cannot have the second, or we would again have $m < n - 1 < n$, so $m < n$. Now if the third holds, then either $m = n$ or $m > n$, which we have assumed is not the case. This proves the assertion, and also shows that $<$ is a total order on $\mathbb{N}$.

Now that we have a solid axiomatic foundation for the natural numbers, we can define addition using what is called the *successor* function S. For any natural number n, we define $S(n) = \{n, \{n\}\}$, which is just the number $n + 1$, the successor to n. We then define addition formally by setting

$n + 0 = n$ for any n, and $n + S(k) = S(n + k)$. Thus

$$\begin{aligned} n+1 &= n + S(0) = S(n+0) = S(n) \\ n+2 &= n + S(1) = S(n+1) = SS(n) \\ n+3 &= n + S(2) = S(n+2) = SSS(n) \\ n+4 &= n + S(3) = S(n+3) = SSSS(n) \\ &\cdots \\ &\text{and so on.} \end{aligned}$$

With this definition, we note that we can always write the number n as $S \ldots S(0)$, where there are n S's. From this it is obvious that addition is *commutative*, meaning that $n + k = k + n$ for any natural numbers n and k, and *associative*, meaning $(n + k) + r = n + (k + r)$ for all $n, k, r \in \mathbb{N}$. This makes the natural numbers into what is called in modern algebra a commutative *semigroup* with identity.

In general, a semigroup is a set G with an associative binary operation R on G, meaning a function $R{:}G \times G \to G$ such that $(aRb)Rc = aR(bRc)$. A semigroup G is commutative if $aRb = bRa$ for all $a, b \in G$, and G has an identity if there is some $i \in G$ such that $aRi = iRa = a$ for all $a \in G$. Semigroups occur a lot in modern mathematics, as we shall see. In the semigroup $\mathbb{N}$, the operation is $+$ and the identity is 0. Moreover, $\mathbb{N}$ is a *commutative* semigroup because for $m, n \in \mathbb{N}$, we have $m + n = n + m$. and it is an *ordered* semigroup because the total order $<$ satisfies $a, b > 0 \to a + b > 0$. Finally, $\mathbb{N}$ has the *additive unit* 0, which is an element such that for any $n \in \mathbb{N}$, $0 + n = n$.

The natural numbers are also a commutative, ordered semigroup with unit 1 with respect to multiplication. In this case, the semigroup property is that multiplication is associative: $(mn)k = m(nk)$ for any three natural numbers m, n, and k. The semigroup is commutative because $mn = nm$ for any two natural numbers m and n. The unit 1 satisfies $1 \cdot m = m$ for any natural number m. The multiplicative semigroup of natural numbers is totally ordered by $<$, and the order is compatible with multiplication because $m, n > 0$ implies $mn > 0$.

4.4 Proving the Obvious

The reader may have been hoodwinked by my handwaving about the "number of S's" that I actually proved that addition in $\mathbb{N}$ really is commutative

and associative. Formally, however, this was no proof at all, and I at least am left with the knawing feeling that I may have glossed over some important points. So the impatient reader can skip this section, but the curious may be rewarded by going through the full argument. This argument, inspired by Kahn (2007), uses lots mathematical induction, as developed in section 3.6.

First we show that for any natural numbers l, m, and n, we have

$$\begin{aligned} m + 0 &= 0 + m; && (4.1)\\ m + 1 &= 1 + m; && (4.2)\\ l + (m + n) &= (l + m) + n. && (4.3)\\ m + n &= n + m. && (4.4) \end{aligned}$$

For (4.1), by definition $m + 0 = m$, so we must show that $0 + m = m$ for all natural numbers m. First, $0 + 0 = 0$ by definition. Suppose $0 + m = m$ for all natural numbers less than or equal to k. Then

$$\begin{aligned} 0 + S(k) &= S(0 + k) && \text{definition of addition}\\ S(0 + k) &= S(k) && \text{induction assumption} \end{aligned}$$

By induction, (4.1) is true for all natural numbers.

For (4.2), $m + 1 = m + S(0) = S(m + 0) = S(m)$, so we must show $1 + m = S(m)$. This is true for $m = 0$ by (4.1), so suppose it is true for all natural numbers less than or equal to k. Then $1 + S(k) = S(1 + k) = S(k + 1) = S(S(k))$. The first equality is by definition, the second by the induction assumption, and the third by definition. By induction, (4.2) is true for all natural numbers.

For (4.3), to avoid excessive notation, we define the predicate $P(n)$ to mean

$$(\forall l, m)(l + (m + n) = (l + m) + n),$$

and we prove $(\forall n)(P(n))$ by induction. For $n = 0$, $P(0)$ says

$$(\forall l, m)(l + (m + 0) = (l + m) + 0),$$

which, from the previous results, can be simplified to

$$(\forall l, m)(l + m = l + m),$$

which is of course true. Now suppose $P(n)$ is true for all n less than or equal to k. Then $P(S(k))$ says that for all l, m,

$$l + (m + S(k)) = (l + m) + S(k),$$

which can be rewritten as

$$l + S(m + k) = S((l + m) + k),$$

and then as

$$S(l + (m + k)) = S(l + (m + k)),$$

using the induction assumption. The final assertion is true, so $P(S(k))$ is true, and the result follows by induction. I will leave the final assertion, the law of commutativity of addition as an exercise for the reader.

4.5 Multiplying Natural Numbers

We can define multiplication in $\mathbb{N}$ recursively, as follows. For any natural number n, we define $0 \cdot m = 0$, and if we have defined $k \cdot m$ for $k = 0, \ldots, n$, we define $(n+1) \cdot m = n \cdot m + m$. Note that we have used addition to define multiplication, but this is valid, since we have already defined addition for natural numbers.

With this definition, the multiplication has the following properties, where $m, n, k, l \in \mathbb{N}$.

1. Distributive law: $k(m + n) = mk + nk = (m + n)k$
2. Associative law: $(mn)k = m(nk)$
3. Commutative law: $mn = nm$
4. Multiplicative order: $m \leq n$ if and only if $lm \leq ln$
5. Multiplicative identity: $1 \cdot m = m$.

To prove the distributive law, note that for any natural numbers k and m, it holds for $n = 0$. Suppose it is true for $n = 0, \ldots, r$. Then we have

$$\begin{aligned} k(m + (r + 1)) &= k((m + r) + 1) = k(m + r) + m + r \\ &= km + kr + m + r = k(m + 1) + k(r + 1), \end{aligned}$$

where we have freely used the associative and distributive laws for addition. By induction, the first half of the distributive law is proved. The second half of the distributive law is proved similarly.

To prove the associative law, note that for any m and n, $(mn)\cdot 0 = 0$ while $m(n \cdot 0) = m \cdot 0 = 0$, so the associative law is true for $k = 0$. Suppose it is true for $k = 0, \ldots, r$. Then we have

$$\begin{aligned}(mn)(r+1) &= (mn)r + mn = m(nr) + mn \\ &= m(nr + n) = m(n(r+1)),\end{aligned}$$

where we have used the distributive law for multiplication, which we have already proved.

To prove the commutative law, note that for any m, $m \cdot 0 = 0 \cdot m = 0$. so the commutative law is true for $n = 0$. Suppose it is true for $n = 0, \ldots, r$. Then we have

$$m(n+1) = (mn) + m = nm + m = (n+1)m,$$

where we have used the second form of the distributive law.

I leave it to the reader to prove the fina two of the above properties.

4.6 The Integers

It is a drag not to be able to define subtraction for any two natural numbers, so we define a new set of numbers, called the *integers*

$$\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

We can define an integer explicitly as either $+n$ or $-n$, where $n \in \mathbb{N}$. We can do this by defining two new symbols, "+" and "-", and letting $+n$ be the ordered pair $(+, n)$ and $-n$ be the ordered pair $(-, n)$, where $n \in \mathbb{N}$. We can conserve on symbols by defining $+n$ to be the ordered pair $(1, n)$ and defining $-n$ to be the ordered pair $(0, n)$, where $n \in \mathbb{N}$. Either way, we assume $+0 = -0$, which denote simply by 0, and we identify the integer $+n$, naturally enough, with the natural number n. We can define addition of integers easily in terms of addition and subtraction of natural numbers.

The definition goes like this (check it out!), where $m, n \in \mathbb{N}$:

$$\begin{aligned}
+n + +m &= +(n+m) \\
-m + -n &= -(m+n) \\
+n + -m &= \begin{cases} +(n-m) & \text{for } n \geq m \\ -(m-n) & \text{for } m \geq n \end{cases} \\
+n - +m &= +n + -m \\
+n - -m &= +n + +m \\
-n - +m &= -n + -m \\
-n - -m &= -n + +m.
\end{aligned}$$

We also define a new operation on integers, called *negation*, which goes $-+n = -n$ and $--n = +n$. With this new operation, we can shorten the definition of integer subtraction to $i - j = i + (-j)$ where i and j are integers, so the last four lines in (4.5) to a single line. For instance, $+n--m = +n+-(-m) = +(n+m)$. We must also define multiplication of integers. We say

$$+m \cdot +n = -m \cdot -n = +mn \tag{4.5}$$

$$+m \cdot -n = -m \cdot +n = -mn \tag{4.6}$$

This looks very complicated, but it is in fact probably how you learned to subtract integers in school. You can check as an exercise that (a) subtraction is defined for all integers; (b) $+0 = -0$ is an additive identity for integers; (c) integer addition is commutative; (d) the distribution law for multiplication over addition holds for integers; and (e) for any two integers i and j, we have $i - j = -(j - i)$. When there is no confusion, we write n instead of $+n$ for the integer $+n$; i.e., nonnegative integers (integers without the minus sign) are identified with natural numbers.

When we get to abstract algebra later, you will see that the integers form a *commutative group* with respect to addition.

Note that $\mathbb{Z}$ has the same cardinality as $\mathbb{N}$. To see this, note that $f : \mathbb{N} \to \mathbb{Z}$ given by $f(k) = +k$ for $k \in \mathbb{N}$ is an injection, and $g(0) = 0$, $g(+k) = 5k$, and $g(-k) = 2^k$ is an injection from $\mathbb{Z}$ to $\mathbb{N}$, so by the Cantor-Bernstein Theorem, there is a bijection between $\mathbb{Z}$ and $\mathbb{N}$ (actually, it is easy to construct a bijection directly—try it).

We write the cardinality of $\mathbb{N}$, following Cantor, as $\aleph_0$.

There is a quite different way of deriving the integers from the natural numbers that the reader might like to explore. Let integers be natural number pairs (m,n) and treat two such numbers (m,n) and (m',n') as equal if $n+m'=n'+n$. With this scheme, $(m,m)=(0,0)$, which we call the additive unit of the integers (zero). We then add these integers term by term, so $(m,n)+(m',n')=(m+m',n+n')$. With this definition of addition , we have $(m,n)+(n,m)=(m+n,n+m)=(0,0)$, so for any two natural numbers m and n, the integers (m,n) and (n,m) are negatives each other. if we define $(m,n)>(0,0)$ if $n>m$, then the natural numbers appear in the integers as $(0,0),(0,1),(0,2),\ldots$ and then negative numbers are $\ldots(3,0),(2,0),(1,0)$. Generally, (m,n) is positive, and equal to $(0,n-m)$, if $m<n$ and is negative, and equal to $(m-n,0)$, if $m>n$.

With this system of integers, we define multiplication by $(m,n)\cdot(m',n')=(n'n+m'm,m'n+n'm)$. If you try this out in a few cases (e.g., two positive integers or two negative integers), you will see that it works, and you can prove all the laws of multiplication (associativity, commutativity, the multiplicative unit is $(0,1)$, and the order $<$ is such that if (m,n) and $(m',n')>0$, then $(m,n)\cdot(m',n')>0$).

4.7 The Rational Numbers

Integers are pretty wonderful, but you can't define division properly on the integers $\mathbb{N}$. What, for instance, is $3/4$? This is why we define a new number, which call a *rational number*, consisting of an ordered pair of integers (i,j), where $i,j\in\mathbb{Z}$ and $j\neq 0$. We think of the first number i as the *numerator* and j as the *denominator*. Formally, we identify $(i,1)$ with the integer i, and we consider two rational numbers (i,j) and (k,l) to be the same if $il=jk$, which means they have the same reduced form in which the denominator does not divide the numerator. Moreover, we define addition of rational numbers by specifying that $(i,j)+(k,r)=(ir+jk,jr)$, and we define multiplication by $(i,j)\cdot(k,r)=(ij,kr)$. Subtraction is defined as $(i,j)-(k,r)=(i,j)+(-k,r)$, Division is defined by $(i,j)/(k,r)=(i,j)\cdot(r,k)$, provided $j,k\neq 0$.

You should check that this definition does not depend on any particular representation of the rational numbers. For instance

$$(im,jm)+(kn,rn)=(imrn+jnkm,jmrn)=(ir+jk,jr),$$

for any non-zero integers m and n, so addition is well defined.

Using terms from modern algebra, the rationals, which we denote by $\mathbb{Q}$, form a commutative group under addition, the non-zero rationals form a commutative group under multiplication, and addition is distributive with respect to multiplication (i.e., $a(b+c) = ab + ac$ for all $a, b, c \in \mathbb{Q}$). We call such an algebraic structure a *field*. There is also a natural total ordering on $\mathbb{Q}$, where $a/b < c/d$ for integers a, b, c, d with b and d nonzero, exactly when $ad < bc$. You can check that with this definition, (a) the ordering agrees with the usual ordering on the integers; and (b) the ordering is trichotomous and transitive. Moreover, if $0 < a$ and $0 < b$, then $0 < ab$;i.e., the product of positive numbers is positive. We call such a field an *ordered field*. $\mathbb{Q}$ is an ordered field.

To prove all of these statements is rather tedious and not very informative, as we use exactly the same techniques as in dealing with the natural numbers and the integers. So, I'll leave this to the curious reader to work out.

4.8 The Algebraic Numbers

The great Greek mathematicians, the Pythagoreans, believe that all positive numbers were rational; i.e., ratios of natural numbers, and even made this belief a part of their world view. Were they correct, the field $\mathbb{Q}$ of rational numbers would be the same as the field $\mathbb{R}$ of real numbers. However, the fifth century BC Pythagorean Hippasus proved that it cannot be the case that $\sqrt{2}$ is the ratio of whole numbers. The proof is very beautiful, and can be expressed in just a few lines, using *reductio ad absurdum*.

Suppose $\sqrt{2} = a/b$, where a and b are non-zero natural numbers. If a and b have any common factors, we divide them out, so we can assume they have no common factors. Then squaring both sides, we have $2 = a^2/b^2$, so $2b^2 = a^2$. Thus 2 divides a^2, and since 2 is a prime number (it has no divisors except 1 and itself), 2 must divide a; say $a = 2c$. Then $a^2 = 4c^2$, so $2b^2 = 4c^2$, which reduces to $b^2 = 2c^2$. But then b^2 must be divisible by 2, so b itself must be divisible by 2. We have thus shown that both a and b are divisible by 2, contradicting our assumption that a and b have no common factors.

We call numbers like $\sqrt{2}$ *irrational* because they are not rational. What do we mean by "numbers like" $\sqrt{2}$. Well, $\sqrt{2}$ is a solution, also called a *root*, of the quadratic equation $x^2 - 2 = 0$. In general the roots of polynomial equations

$$ax^n + bx^{n-1} + \ldots + cx + d = 0 \tag{4.7}$$

will fail to be rational numbers. We call the roots of polynomial equations with rational coefficients *algebraic* numbers.

Another problem with the solution of polynomial equations is that they may appear not to exist! For instance, the equation $x^2+2=0$ surely cannot have any real number as its root, because the left hand side is never smaller than 2! Some smart fellow responded to this by defining the *imaginary number* $\mathbf{i} = \sqrt{-1}$. If this is legitimate, and if $\mathbf{i}$ acts in every other respect like a number, so you can do arithmetic with it, then $\mathbf{i}\sqrt{2}$ is a root of the equation $x^2 + 2 = 0$, and $-\mathbf{i}\sqrt{2}$ is a second root. Indeed, if we admit the imaginary number $\mathbf{i}$, then we have a whole new algebra of *complex numbers* of the form $a+b\mathbf{i}$ where a and b are rational or irrational numbers. Complex numbers were first used by the Italian mathematician Gerolamo Cardano in the mid-sixteenth century.

The arithmetic of complex numbers is given by

$$\begin{aligned}
(a+b\mathbf{i}) + (c+d\mathbf{i}) &= (a+c) + (b+d)\mathbf{i} \\
(a+b\mathbf{i}) - (c+d\mathbf{i}) &= (a-c) + (b-d)\mathbf{i} \\
(a+b\mathbf{i}) \cdot (c+d\mathbf{i}) &= (ac-bd) + (ad+bc)\mathbf{i} \\
\frac{a+b\mathbf{i}}{c+d\mathbf{i}} &= \frac{ac+bd}{c^2+d^2} + \frac{ad-bc}{c^2+d^2}\mathbf{i}.
\end{aligned}$$

These rules are all pretty obvious, except perhaps the last, which we get by multiplying the numerator and denominator of the left hand side by $c - d\mathbf{i}$ and simplifying.

Complex numbers are wonderful, for they give us the following theorem, the so-called Fundamental Theorem of Algebra.

THEOREM 4.1 Fundamental Theorem of Algebra: *The polynomial*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

with $a_i \in \mathcal{C}$ *can be factored as*

$$p(x) = a(x-r_1)\ldots(x-r_n)$$

where a *is a constant and each* r_i *is a complex number. The* $\{r_i\}$ *are unique, except for their order of appearance in the above expression.*

The Fundamental Theorem of Algebra is often expressed as saying that every n-degree polynomial has exactly n roots. This is true if we allow for

repeated roots. Another way of expressing the Fundamental Theorem is that the field $\mathcal{C}$ of complex numbers is *algebraically closed*.

But, is it legal just to invent a convenient new number $\mathbf{i}$? There was much controversy about this a few centuries ago, which is why the term "imaginary" was applied to them (and the name has stuck). However, another smart fellow showed that one could define complex numbers directly as ordered pairs of real numbers with the appropriate rules for arithmetic. We write $(a, 0)$ for real numbers and $(0, b)$ for imaginary numbers, so the complex number $a + b\mathbf{i}$ becomes (a, b). We then define arithmetic on complex numbers by

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) - (c, d) = (a - c, b - d)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

and

$$\frac{a + b\mathbf{i}}{c + d\mathbf{i}} = \frac{(ac + bd) + (bc - ad)\mathbf{i}}{c^2 + d^2}.$$

The complex numbers thus form a field (it is easy to check that the distributive law holds for $\mathbb{Q}$). However, they do not form an ordered field. To see this, suppose $\mathbf{i} > 0$. Then $-1 = \mathbf{ii} > 0$, which is false. Thus we must have $-\mathbf{i} > 0$, so $-1 = (-\mathbf{i})(-\mathbf{i}) > 0$, which is also false. It follows that no total order can be defined on the field of complex numbers that is compatible with the algebraic operations (i.e, for which the product of two positive numbers is positive).

4.9 Proof of the Fundamental Theorem of Algebra

Suppose a polynomial $p(x)$ of degree n with coefficients in $\mathcal{C}$ does not have a root in $\mathcal{C}$. We may assume $p(x)$ has real coefficients, using the following argument.

If $z = x + \mathbf{i}y$ is a complex number, $x, y \in \mathbf{R}$, we define the *complex conjugate* $x - \mathbf{i}y$ of z as $\overline{z}$. Clearly if z is a real number, then $z = \overline{z}$, and in general $z\overline{z} = x^2 + y^2$, which is often written as $|z|^2$, the square of the *modulus* $|z|$ of z. It is also clear that $\overline{\overline{z}} = z$ for any complex number z, and $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$. Moreover, if $p(z)$ is a polynomial with complex coefficients, then $q(z) = p(z)\overline{p(\overline{z})}$ has real coefficients, and a root w of $q(z)$ is either a root of $p(z)$ or $\overline{w}$ is a root of $p(\overline{z})$, in which case $\overline{w}$ is a root of $p(z)$. To

show that $q(z)$ has real coefficients, we assume z is real and we show that $q(z) = \overline{q}(z)$. We then have

$$\overline{q}(z) = \overline{p(z)\overline{p(\overline{z})}} = \overline{p(z)}\,\overline{\overline{p(\overline{z})}} = \overline{p(z)}p(z) = q(z),$$

which proves the assertion.

Now we assume $p(x)$ has real coefficients and of odd degree. Then for sufficient large x, $p(x)$ and $p(-x)$ have opposite signs, because the polynomial has the same sign as its term of highest degree for sufficiently large $|x|$ (i.e., for large positive or large negative x). To see this, suppose $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Then, dividing by x^n, we get

$$\frac{p(x)}{x^n} = a_n + \frac{a_{n-1}}{x} + \ldots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n},$$

which must have the same sign as a_n for large x.

To prove that $p(x)$ has a root, we will use a very famous theorem from the calculus, called the *Intermediate Value Theorem*. This theorem says that if a polynomial $p(x)$ with real coefficients and x a real variable, changes sign between $x = a$ and $x = b > a$, then $p(x) = 0$ for some $x \in (a, b)$.[1] We prove this theorem in §7.2.

Clearly, using the Intermediate Value Theorem, the assertion that a polynomial of odd degree has a real root is immediately proved by the above reasoning. The interesting thing about this proof is that it is not algebraic, but depends on the properties of the real line, in particular its *completeness*, which we will define in section 4.10.

Thus if $p(x)$ has odd degree, it has a root r. But then it is easy to show that $p(x) = (x - r)q(x)$ where $q(x)$ is a polynomial of one degree less than $p(x)$. This fact, by the way, does not depend on the fact that $p(x)$ has odd degree, which shows that we can prove the Fundamental Theorem by mathematical induction: it is true for polynomials of degree one, and if it is true for polynomials of degree n, then it is true for polynomials of degree $n + 1$. However, we have only showed that it is true for polynomials of odd degree. We must deal with polynomials of even degree. If a polynomial of even degree n has a root r, it factors into $(x - r)$ times a polynomial of odd degree $n - 1$, which then factors into $(x - s)$ times another polynomial of

[1]Recall that (a, b) means $\{r \in \mathbf{R} | a < r < b\}$. By the way, the intermediate value theorem is true for any continuous function, but we have not yet defined the notion of a *continuous function*.

even degree $n-2$. So, we only need deal show that a polynomial of even degree has a root.

But, before we continue with the proof, let's see why if r is a root of $p(x)$, then $p(x) = (x-r)q(x)$ for some polynomial $q(x)$. Suppose

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

has root r. Then

$$p(r) = a_n r^n + a_{n-1}r^{n-1} + \ldots + a_1 r + a_0 = 0.$$

Subtracting the last equation from the previous, we get

$$p(x) = a_n(x^n - r^n) + a_{n-1}(x^{n-1} - r^{n-1}) + \ldots + a_1(x-r).$$

However, for any integer k, we have

$$\frac{x^k - r^k}{x-r} = x^{k-1} + x^{k-2}r + x^{k-3}r^2 + \ldots + xr^{k-2} + r^{k-1}.$$

Thus

$$\frac{p(x)}{x-r} = a_n\frac{x^n - r^n}{x-r} + a_{n-1}\frac{x^{n-1} - r^{n-1}}{x-r} + \ldots + a_1$$

is a polynomial.

This leaves us to deal with polynomials of even degree. Clearly $p(x) = ax^2 + bx + c$, which is of degree 2, has two roots given by the well-known formula

$$x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

So suppose $p(x)$ is of degree $2^n m \geq 4$ where m is odd and we have proven the theorem for all polynomials of degree less than or equal to $2^{n-1}m$. First, we form the vector space $\mathcal{C}[x]$, where x is a variable, with typical element $r_0 + r_1 x + r_2 x^2 + \ldots + r_n x^n$, where $r_0, \ldots, r_n \in \mathcal{C}$. We define addition by

$$(r_0 + r_1 x + r_2 x^2 + \ldots + r_n x^n) + (s_0 + s_1 x + s_2 x^2 + \ldots + s_m x^m) =$$

$$(r_0 + s_0) + (r_1 + s_1)x + \ldots (r_n + s_n)x^n + s_{n+1}x^{n+1} + \ldots + s_m x^m,$$

where $n \leq m$.

Now for any vector $\mathbf{v} \in \mathcal{C}[x]$ we let $[\mathbf{v}]$ be the remainder when we divide $\mathbf{v}$ by the polynomial $p(x)$; i.e., if $\mathbf{v} = p(x)q(x) + r(x)$, where the polynomial

$r(x)$ has degree less than the degree n of $p(x)$, then $[\mathbf{v}] = r(x)$. Now it is easy to show that the set of new vectors $[\mathbf{v}]$ for $\mathbf{v} \in \mathcal{C}[x]$ is itself a vector space $\mathcal{C}[x]_p$ of dimension $n-1$ and basis vectors $[1], [x], [x^2], \ldots, [x^{n-1}]$. Because $\mathcal{C}[x]_p$ is $n-1$ dimensional, we can write

$$1 = r_0[x] + r_1[x]^2 + \ldots + r_{n-1}[x^{n-1}] + r_n[x^n],$$

for some $r_0, \ldots, r_n$, where $r_n \neq 0$ because any n vectors in $\mathcal{C}[x]_p$ are linearly dependent. We can write this as

$$1 = [x](r_0 + r_1[x] + \ldots + r_{n-1}[x^{n-2}] + r_n[x^{n-1}]),$$

which shows that

$$1/[x] = r_0 + r_1[x] + \ldots + r_{n-1}[x^{n-2}] + r_n[x^{n-1}].$$

That is, $\mathcal{C}[x]_p$ is actually a field, with $\mathcal{C}$ as a subfield By construction $p([x]) = 0$ in this field. That is, $[x]$ is a root of $p(x)$ in $\mathcal{K} = \mathcal{C}[x]_p$.

In this new field $\mathcal{K}$, the polynomial p factors into $p_1(x)(x - [x])$. Now factor $p_1(x) \in \mathcal{P}(\mathcal{K})$, the polynomials over field $\mathcal{K}$. If $p_1(x)$ does not factor into linear terms, let $p_2(x)$ be any nonlinear factor of $p_1(x)$, and construct a new field $\mathcal{K}_1$ over $\mathcal{K}$ where $p_2(x)$ has a root. It is clear that this new root is also a root of $p(x)$, so now we have found a superfield $\mathcal{K}$ of $\mathcal{C}$ in which $p(x)$ has at least two roots. We continue this process of contructing superfields until we reach one, say $\mathcal{K}^*$, in which $p(x)$ factors into linear factors, $p(x) = a(x - z_1)(x - z_2)\ldots(x - z_n)$ with $z_i \in \mathcal{K}^*$, and indeed $\mathcal{K}^*$ is simply the complex field $\mathcal{C}$ with the n (including possible repeats) elements $z_1, \ldots, z_n$ adjoined.

The *elementary symmetric polynomials* in variables $x_1, \ldots, x_n$ are of the form

$$\begin{aligned}
e_0(x_1, \ldots, x_n) &= 1 \\
e_1(x_1, \ldots, x_n) &= \sum_{i=1}^{n} x_i \\
e_2(x_1, \ldots, x_n) &= \sum_{i,j=1, i \leq j}^{n} x_i x_j \\
e_3(x_1, \ldots, x_n) &= \sum_{i,j,k=1, i \leq j \leq k}^{n} x_i x_j x_j \\
&\ldots \\
e_n(x_1, \ldots, x_n) &= x_1 x_2 \ldots x_n.
\end{aligned}$$

To see what this means, you should write out (4.8) for a few values of n. In a professional article or book, the author may not do that for you, and most likely will not instruct you to do so either. Here are some examples:

$n = 1$:
$e_1(x_1) = x_1;$

$n = 2$:
$e_1(x_1, x_2) = x_1 + x_2;$
$e_2(x_1, x_2) = x_1 x_2;$

$n = 3$:
$e_1(x_1, x_2, x_3) = x_1 + x_2 + x_3;$
$e_2(x_1, x_2, x_3) = x_1 x_2 + x_1 x_3 + x_2 x_3;$
$e_3(x_1, x_2, x_3) = x_1 x_2 x_3;$

$n = 4$:
$e_1(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4;$
$e_2(x_1, x_2, x_3, x_4) = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4;$
$e_3(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4;$
$e_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4.$

The reason we introduce the elementary symmetric polynomials is that if $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ has roots $r_1, \ldots, r_n$ and has leading coefficient 1, then we can write

$$\begin{aligned} p(x) \;=\; & x^n + e_1(r_1, r_2, \ldots, r_n) x^{n-1} + e_2(r_1, r_2, \ldots, r_n) x^{n-2} + \ldots \\ & + e_{n-1}(r_1, r_2, \ldots, r_n) x + e_n(r_1, r_2, \ldots, r_n). \end{aligned}$$

In other words, $a_i = e_i(r_1, \ldots, r_n)$ for $i = 1, \ldots, n$.

We prove below that every symmetric polynomial $P(z_1, \ldots, z_n)$ in $\mathcal{K}^*$ can be written as a polynomial $Q(e_1(z_1, \ldots, z_n), \ldots, e_n(z_1, \ldots, z_n))$; i.e., any symmetric polynomial is a polynomial function of the elementary symmetric polynomials. This assertion is called the *Fundamental Theorem of Symmetric Polynomials*. Using this theorem, and taking into account (4.8), we can write $P(z_1, \ldots, z_n)$ as $Q(a_1, \ldots, a_n)$; i.e., we can assume P has its coefficients in the base field $\mathcal{C}$.

Consider, then the polynomial

$$q(z) = \prod_{1 \le i < j \le n} (z - z_i - z_j + t z_i z_j)$$

where t is a real number. This polynomial over $\mathcal{K}^*$ is symmetric in the $\{z_i\}$, so its coefficients are real numbers, being functions of $a_1, \ldots, a_n$. The

degree of this polynomial is $mn(n-1)/2 = 2^{k-1}(n-1)m$ and $m(n-1)$ is an odd number, so $q(z)$ has a complex root by the induction assumption. Indeed, because there are an infinite number of possible t's, we can find two real numbers, s and $t \neq s$, such that $z_i + z_j + t z_i z_j$ and $z_i + z_n + s z_i z_j$ are both complex. Subtracting one from the other, we see that $z_i z_j$ is complex, and subtracting s times the first from t times the second, we see that $z_i + z_j$ is complex. However z_i and z_j are roots of the second degree polynomial $x^2 - (z_i + z_j)x + z_i z_j$, which we know has complex roots. Therefore z_i and z_j are complex numbers. Now dividing $p(x)$ by $(x - z_i)(x - z_j)$, we obtain a lower degree polynomial, which can be factored by the induction assumption.

To prove the Fundamental Theorem of Symmetric Polynomials, we take an approach inspired by David Jao's entry on PlanetMath.org, "Reduction Algorithm for Symmetric Polynomials." The symmetric polynomical $P(x_1, \ldots, x_n)$ is a sum of monomials of the form $c x_1^{i_1} \ldots x_n^{i_n}$, where the i_j are nonnegative integers and c is a complex constant. We define a total order on the monomials by specifying that

$$c_1 x_1^{i_1} \ldots x_n^{i_n} < c_2 x_1^{j_1} \ldots x_n^{j_n} \tag{4.8}$$

if $c_2 \neq 0$ and there is some $k < n$ such that $i_{n-l} = j_{n-l}$ for $l = 0 \ldots k$ but $i_{k+1} < j_{k+1}$. For instance $(2, 3, 4) < (6, 4, 5)$ and $(3, 4, 5) < (4, 4, 5)$. In words, starting in the n^{th} position in both monomials, go back until the two exponents are not equal. The monomial with the larger exponent in that position is the larger monomial. This is called a *lexicographic order* on the monomials.

We reduce P into elementary symmetric polynomials by successively subtracting frmon P a product of elementary symmetric polynomials eliminating the largest monomial according to this order without introducing any larger monomials. This way, in each step, the largest monomial becomes smaller and smaller until it becomes zero, and we are done: the sum of the subtracted-off polynomials is the desired expression of P as a polynomial function of elementary polynomials.

Suppose $c x_1^{i_1} \ldots x_n^{i_n}$ is the largest monomial in P. Consider the polynomial $P_1 = P - Q$, where

$$Q := c s_1^{i_n - i_{n-1}} s_2^{i_{n-1} - i_{n-2}} \ldots s_{n-1}^{i_2 - i_1} s_n^{i_1}$$

and s_k is the k^{th} elementary symmetric polynomial in the n variables $x_1, \ldots, x_n$. Clearly Q is a polynomial in the symmetric polynomials. Moreover, x_n occurs with exponent i_n, since it occurs with exponent $i_n - i_{n-1}$ in

the first term, $i_{n-1} - i_{n-2}$ in the second term, and so on, down to i_1 times in the final term. Moroever, $x_n^{i_n}$ only occurs in a single monomial in Q, and in that monomial, x_{n-1} occurs with exponent i_{n-1}, since it does not include a term from s_1, and it occurs in the rest of Q with exponent $i_{n-1} - i_{n-2}$ in the second term, $i_{n-2} - i_{n-3}$ in the third term, and so on, down to i_1 times in the final term. And so on for the remaining variables. This shows that $P - Q$ has monomials that are smaller than the one just eliminated. We can now continuous the process until nothing remains in P.

As I have stressed throughout this book, to understand a complex argument, go through a few simple cases yourself. Here is one example of the above algorithm. Suppose $P(x_1, x_2) = (x_1 + 7x_1x_2 + x_2)^2$. Expanding this into monomials, we get

$$P = x_1^2 + 2x_1x_2 + 14x_1^2x_2^2 + x_2^2 + 14x_1x_2^2 + 49x_1^2x_2^2.$$

The largest monomial is $49x_1^2x_2^2$, so we subtract off $49s_2^2$, getting

$$P - 49s_2^2 = x_1^2 + 2x_1x_2 + 14x_1^2x_2 + x_2^2 + 14x_1x_2^2.$$

Now the largest monomial is $14x_1x_2^2$, so we subtract off $14s_1s_2$, getting

$$P - 49s_2^2 - 14s_1s_2 = x_1^2 + 2x_1x_2 + x_2^2$$

Now the largest monomial is x_2^2, so we subtract off s_1^2, getting

$$P - 49s_2^2 - 14s_1s_2 - s_1^2 = 0.$$

This gives

$$P(x_1, x_2) = 49s_2(x_1, x_2)^2 + 14s_1(x_1, x_2)s_2(x_1, x_2) + s_1(x_1, x_2)^2.$$

4.10 The Real Numbers

We have define complex and algebraic numbers in terms of real numbers. But we have not defined real numbers! If you check over previous sections of this and the previous chapter, you will see that we have defined everything ultimately in terms of the empty set $\emptyset$, using the axioms of set theory. But the moment we discovered the first irrational number, we entered a novel domain of mathematics. How can we define the real numbers?

A beautiful definition of the reals in terms of the rationals was discovered by the great nineteenth century German mathematician Julius Wilhelm

Richard Dedekind. Note that $\sqrt{2}$ is the smallest number greater than any number in the set

$$D(r^2 < 2) = \{q \in \mathbb{Q} | q^2 < 2\}. \tag{4.9}$$

So, why not simply define $\sqrt{2}$ as $D(r^2 < 2)$? In effect, this would be saying that $\sqrt{2}$ is the least upper bound of the set of rational numbers extending from $-\infty$ up to, but not including $\sqrt{2}$. We define a number u to be an *upper bound* of a set A of numbers if $u \geq a$ for all $a \in A$. We say u is the *least upper bound* of the set A if it is the smallest number that is an upper bound of A. Note that a set like $D(r^2 < 2)$ defined in (4.9) has an upper bound in $\mathbb{Q}$, indeed lots of them, but it has no *least* upper bound; for every upper bound $u \in \mathbb{Q}$, there is a still smaller upper bound. Thus, considering sets of rational numbers, the least upper bound need not exist, as is the case of $D(r^2 < 2)$. For convenience, we define lub$A$ as the least upper bound of the set A.

For future reference, we say l is a *lower bound* for a set A of numbers if $l \leq a$ for all $a \in A$, and we say l is the *greatest lower bound* of A if l is a lower bound of A and any other lower bound of A is smaller than A. We write glb$A$ for the greatest lower bound of A.

Note that if $q \in \mathbb{Q}$, q is the least upper bound of the set

$$D(r < q) = \{r \in \mathbb{Q} | 0 \leq r < q\}.$$

The main difference between $D(r < q)$ and $D(r^2 < 2)$ is that at the upper end of the latter set there is a "hole" because $\sqrt{2}$ is not rational, while lub$D(r < q) = q$ when $q \in \mathbb{Q}$.

If we can work out the details of how to add, subtract, multiply and divide numbers that look like $D(r^2 < 2)$, and if the resulting algebraic system has the properties we normally associated with the real numbers, we will have effectively define $\mathbb{R}$, the real numbers. Formally, we want the real numbers $\mathbb{R}$ to be a totally ordered field in which every set with an upper bound in $\mathbb{R}$ has a least upper bound in $\mathbb{R}$. Moreover, we want the mapping that takes $q \in \mathbb{Q}$ into $D(r < q) \in \mathbb{R}$ to be an *isomorphism*, which means an injection that preserves all the algebraic operations (e.g., $D(r < q) + D(r < q') \mapsto D(r < q + q')$, for $q, q' \in \mathbb{Q}$).

We thus define a nonnegative real number as a set α of rational numbers such that

1. α is non-empty;

2. α has an upper bound; i.e., $(\exists u \in \mathbb{Q})(a \in \alpha \rightarrow a < u)$;
3. α has no negative upper bound; i.e.,
   $(\forall a \in \alpha)((a < 0) \rightarrow (\exists a' \in \alpha)(a < a'))$;
4. Negative Tail property: $(\forall x, y \in \mathbb{Q})(x < y \wedge y \in \alpha \rightarrow x \in \alpha)$;
5. α has no largest element; i.e., $(\forall a \in \alpha)(\exists a' \in \alpha)(a' > a)$.

We call any such set a *Dedekind cut*. A Dedekind cut contains all rational numbers from $-\infty$ to any rational number in the cut. The reason for condition 3 is that, for now, we want to define only non-negative real numbers. Note that condition 5 does not imply that a real number has no least upper bound, but it requires that a real number cannot *contain* its least upper bound, should it have one.

By the way, I am now freely using the notation we developed in chapters 2 and 3. I hope you feel comfortable with them by now. This does not mean you should be able to read the previous definition with the ease that you read the morning headlines in the newspaper. It means, rather, that with some thought, effort, and time, and perhaps by reviewing some of the earlier material in the book, the definition of a Dedekind cut becomes clear to you. If not, you should restart your reading of the book back at some earlier point. I freely admit that I do this all the time in reading mathematical material.

We now define a non-negative *real number* as a Dedekind cut α. We turn the real numbers into an algebraic structure much like $\mathbb{N}$ by defining addition, multiplication, and division as well as the identity element for addition (zero) and for multiplication (one). We will call this $\mathbb{R}$. We then define negative real numbers and subtraction in the same way we defined negative integers in section 4.6. In this way, we construct the field $\mathbb{R}$ of real numbers, which will also be an ordered field, with the order conforming to our definitions of positive and negative.

First we note that the real numbers $\mathbb{R}$ can be totally ordered by set inclusion, so we write $\alpha < \beta$ if $\alpha \subset \beta$. We then define the additive identity of the real numbers by $0_{\mathbb{R}} = \{q \in \mathbb{Q} | q < 0\}$, and we define the multiplicative identity by $1_{\mathbb{R}} = \{q \in \mathbb{Q} | q < 1\}$. Note that $0_{\mathbb{R}} < 1_{\mathbb{R}}$, as required if $\mathbb{R}$ is to follow the normal laws of arithmetic.

We define addition of real numbers by

$$\alpha + \beta = \{x + y | (x \in \alpha) \wedge (y \in \beta)\}.$$

The first thing we must check is that $\alpha + \beta$ is a real number; i.e., it is a Dedekind cut. Let $\gamma = \alpha + \beta$. We must show that γ satisfies all five of the

conditions in the definition of a Dedekind cut. Clearly $\gamma \neq \emptyset$ and γ has an upper bound. Suppose γ has a negative upper bound $u < 0$. Because α has no negative upper bound, there is an $a \in \alpha$ with $a > u/2$. Similarly there is a $b \in \beta$ with $b > u/2$ Thus $a + b \in \gamma$ and $a + b > u$, which shows that u is not an upper bound for γ. This is a contradiction, showing that γ has no negative upper bound. Note that all these calculation are quite legal because they occur in $\mathbb{Q}$, not $\mathbb{R}$.

Now suppose $x, y \in \mathbb{Q}$, $x < y$ and $y \in \gamma$. Then $y = a + b$ for $a \in \alpha$ and $b \in \beta$. Now $x - b < a$, so $x - b \in \alpha$. But then $x = (x - b) + b \in \gamma$. This proves the Negative Tail property.

Finally, suppose $g \in \gamma$ is the largest element of γ. Then $g = a + b$ for $a \in \alpha$ and $b \in \beta$. But there is an $a' \in \alpha$ with $a' > a$, so $g' = a' + b$ is in γ and is larger that g. This *reductio ad absurdum* shows that γ has no largest element. We have thus proved that $\alpha + \beta$ is a real number.

To show that $0_{\mathbb{R}}$ is an additive identity, we must show that for any real number α, we have $\alpha + 0_{\mathbb{R}} = \alpha$. Clearly $\alpha + 0_{\mathbb{R}} \leq \alpha$ (i.e., $\alpha + 0_{\mathbb{R}} \subseteq \alpha$) because if you add a negative rational to $a \in \alpha$, the result must be in α by the Negative Tail property of α. If $a \in \alpha$, there is some $a' \in \alpha$ with $a' > a$. Then $a - a' < 0$, so $a - a' \in 0_{\mathbb{R}}$, from which it follows that $a' + (a - a') = a \in \alpha + 0_{\mathbb{R}}$. Thus we have shown that $\alpha = \alpha + 0_{\mathbb{R}}$.

We define multiplication of nonnegative real numbers by $\alpha\beta = 0_{\mathbb{R}}$ if either α or β is $0_{\mathbb{R}}$, and for $\alpha, \beta > 0_{\mathbb{R}}$,

$$\alpha\beta = \{q \in \mathbb{Q} | q \leq 0\} \cup \{xy | (x \in \alpha) \wedge (y \in \beta) \wedge (x, y > 0)\}.$$

Again, we must first check that $\gamma = \alpha\beta$ is a real number for $\alpha, \beta > 0$. Clearly γ is nonempty and has an upper bound. If both α and β are nonzero, then they must have strictly positive elements $a > 0$ and $b > 0$ (this is because $\{q \in \mathbb{Q} | q \leq 0\}$ is not a real number). Thus $ab \in \gamma$, so γ doesn't have a negative upper bound.

I leave it to the reader to prove that γ has the Negative Tail property, and has no largest element, so γ is a real number.

Note that both addition and multiplication are obviously commutative (i.e., $\alpha + \beta = \beta + \alpha$ and $\alpha\beta = \beta\alpha$). I will show that $\alpha \cdot 1_{\mathbb{R}} = \alpha$, proving that $1_{\mathbb{R}}$ is a multiplicative identity. Clearly $\alpha \leq \alpha \cdot 1_{\mathbb{R}}$ because $a = a \cdot 1$ for any $a \in \alpha$. Now let $a' = a \cdot b$ where $a \in \alpha$, $a > 0$, and $b \in 1_{\mathbb{R}}$, $b > 0$. Then $0 < ab < a$, so $ab \in \alpha$ by the Negative Tail property. This shows that $\alpha = a \cdot 1_{\mathbb{R}}$.

Rather than defining division directly, we define the *inverse* α^{-1} of a positive real number α. We then define $\alpha/\beta = \alpha \cdot \beta^{-1}$ for $\beta > 0$. We define, for $\alpha > 0$,

$$\begin{aligned}\alpha^{-1} &= \{q \in \mathbb{Q} | q \leq 0\} \cup \\ &\quad \{q \in \mathbb{Q} | (q > 0) \wedge (1/q \notin \alpha) \\ &\quad \wedge (\exists q \in \mathbb{Q} - \alpha)(q < 1/r)\}.\end{aligned}$$

This definition is quite typical of what you are likely to see in reading a paper or book with equations. It says that α^{-1} consists of all the non-positive rationals, plus any rational of the form $1/q$ where q is not in a and $1/q$ is not the smallest number in $\mathbb{Q} - \alpha$, which is the set of rationals not in α.

We must show that if α is a positive real number, then $\beta = \alpha^{-1}$ is also a real number, and $\alpha \cdot \beta = 1_{\mathbb{R}}$. Clearly β is non-empty. Because $\alpha > 0_{\mathbb{R}}$, there is an $a \in \alpha$ that is positive. Thus if $1/q \in \beta$, then $1/q < 1/a$, so β has an upper bound. If u is an upper bound for α but not the least upper bound of $\mathbb{Q} - \alpha$, then $u > 0$ and $u \notin \alpha$, so $1/u \in \beta$. But $1/u > 0$, so β does not have a negative upper bound. For the Negative Tail property, suppose q, s in $\mathbb{Q}$, $q < s$, and $s \in \beta$. If $q < 0$ then $q \in \beta$. If $s \leq 0$ then $q < 0$, so $q \in \beta$. So suppose $q, s > 0$. Then $1/s \notin \alpha$ and $1/q > 1/s$, so $1/q \notin \alpha$, so $q \in \beta$, since clearly $1/q$ is not the least element in $\mathbb{Q} - \alpha$.

By the way, I should clue you in that when a mathematician says, "Clearly," followed by assertion, you are expected to figure it out for yourself. It may or may not turn out to be easy to show.

To show that if $\beta = \alpha^{-1}$ then $\alpha\beta = 1_{\mathbb{R}}$, note first that if $a \in \alpha$ and $b \in \beta$, then $b = 1/c$ for some $c \notin \alpha$, so $c > a$ and hence $b = 1/c < 1/a$, so $ab < 1$. Therefore $\alpha\beta \leq 1_{\mathbb{Q}}$. Now let q be any positive rational less than one, so $q \in 1_{\mathbb{R}}$. Note that if $\alpha > 1$, then $\beta < 1$ and conversely (why?) so either $q \in \alpha$ or $q \in \beta$. We assume $q \in \alpha$, leaving the alternative, $q \in \beta$, for the reader to work out. Let $\epsilon = 1 - q$, and choose $s \in \alpha$ sufficiently large that $s > q$ and $s + \epsilon \in \mathbb{Q} - \alpha$, but $s + \epsilon$ is not the smallest element of $\mathbb{Q} - \alpha$. Then $1/(s + \epsilon) \in \beta$ and $q < s/(s + \epsilon) < 1$ (to see that $q < s/(s + \epsilon)$, rewrite the inequality as $q(s + \epsilon) < s$, which is $qs + q(1 - q) < s$, which is $q(1 - q) < s(1 - q)$ which is true since $q < s$ and $1 - q > 0$.

Defining the negative numbers can be accomplished either in a way similar to the way we defined the negative integers in $\mathbb{Z}$ in terms of natural numbers $\mathbb{N}$ in section 4.6, or we can define a negative real number as a set of rationals that satisfy conditions 1,2,4, and 5 of the definition of a Dedekind

cut for non-negative rationals, but may have a negative upper bound. The we define $-\alpha$ for $\alpha > 0_{\mathbb{R}}$ as follows:

$$-\alpha = \{q \in \mathbb{Q} | (-q \notin \alpha) \wedge (\exists r \in \mathbb{Q} - \alpha)(r < -q)\}.$$

I will not develop this way of dealing with negative reals, but if you choose to do so, you must show that the negation operator $\alpha \to -\alpha$ is the additive inverse operation. That is, $-0_{\mathbb{R}} = 0_{\mathbb{R}}$, and $\alpha + (-\alpha) = 0_{\mathbb{R}}$. Moreover, you must show that with this definition of negation, that the real numbers form an ordered field. This means showing that if $\alpha > 0_{\mathbb{R}}$, then $-\alpha < 0_{\mathbb{R}}$.

The most important characterization of the real number system $\mathbb{R}$ are that it is the only complete, ordered, and Archimedean field. We already know that $\mathbb{R}$ is an ordered field. We say a field is *complete* if every set of elements with an upper bound has a least upper bound. We saw that rationals are an ordered field, but not a complete ordered field because sets like $D(r^2 < 2)$ have no least upper bound. We corrected this in $\mathbb{R}$ by defining a least upper bound for such sets of rationals. But, we could have left some "holes" somewhere. In fact, we have not.

To prove the reals are complete, let $\{\alpha_\gamma \in \mathbb{R} | \gamma \in \Gamma\}$ be an arbitrary collection of real numbers, where Γ is some arbitrary set of set of indices. Let $\alpha = \cup_{\gamma \in \Gamma} \alpha_\gamma\}$ be the set-theoretic union of all the α_γ, and suppose all the α_γ have a common upper bound $u \in \mathbb{R}$. We can obviously assume $u \in \mathbb{Q}$, so α is nonempty and has and upper bound. We have dropped the third condition, because we now have both positive and negative reals. To show the Negative Tail condition, assume $r, s \in \mathbb{Q}$, $r < s$, and $s \in \alpha$. Then $s \in \alpha_\gamma$ for some $\gamma \in \Gamma$, so $r \in \alpha_\gamma$, which implies $r \in \alpha$. It is obvious that α has no largest element, because such an element would be in one of the α_γ, where it would be the largest element in α_γ, contradicting the fact that α_γ is a real number.

It remains to show that α as defined above is the least upper bound of the set $\alpha_\Gamma = \{\alpha_\gamma | \gamma \in \Gamma\}$. First, α is clearly and upper bound of this set, and for every $r \in \alpha$, there is a α_γ with $r \in \alpha_\gamma$, so r is not an upper bound of α_Γ.

The term Archimedean field, named after the ancient Greek mathematician Archimedes of Syracuse, is the property of having no inf—initely small quantities, or *infinitesimals*. If r is a real number and n is an integer, we define nr to be $r + \ldots + r$, where the addition occurs n times (note that this is conceptually different from $n \cdot r$; in fact you can prove the two are equal). We say $x > 0$ is an infinitesimal if there is a number $y > x$ such that $nx < y$ all natural numbers n. To show that $\mathbb{R}$ is Archimedean, choose

any positive real numbers α and β, with $\alpha < \beta$. Let $r \in \alpha$ with $r > 0$, and let $v \in \mathbb{Q}$ be an upper bound of β. Then n be an integer larger than v/r. Clearly nr is in $n\alpha$ and $nr > v$, so $n\alpha > \beta$.

Non-Archimedean fields do exist, and can be complete and ordered. They can used to develop standard undergraduate calculus in a quite intuitive way, but we will leave this matter for another time.

4.11 Denumerability and the Reals

Most of the approach to numbers developed in this chapter is due to the German mathematician Georg Cantor, who lived from 1845 to 1918. Cantor first defined cardinal and ordinal numbers, and thought of considering two sets to be of equal size if there is bijection from one to the other. One of the achievements of Cantor's approach is that it supplies a very simple proof that not all numbers are algebraic. The proof goes like this. First recall that an algebraic number is the root of a polynomial with rational coefficients; i.e., a number r such that $p(r) = 0$, where $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ and $a_n > 0$.

By the way, now that we have defined the real numbers rigorously, I will revert to writing the real numbers as $\mathbf{R}$ rather than $\mathbb{R}$. I will also write $0_{\mathbb{R}}$ as 0 and $1_{\mathbb{R}}$ as 1.

I want to show that the algebraic numbers are *denumerable*, which means they are infinite in number but they are countable; i.e., you can put them in one-to-one correspondence with the natural numbers. This fact was very, very shocking to mathematicians when Cantor first proved it, because there appears to be many more algebraic numbers than there are integers. So much for raw intuition.

First, suppose we have n denumerable sets $A_1, \ldots, A_n$, where $n \in \mathbb{N}$. Then the union of these sets, $A = A_1 \cup A_2 \cup \ldots \cup A_n$ can be easily shown to be denumerable. Suppose we arrange each set A_i in one-to-one correspondence with the natural numbers, so the j^{th} element of A_i is written a_i^j. By the way, note that we are here using *superscripts* for the first time. The superscript j in a_i^j does not mean the j^{th} power of a_i but rather the j^{th} element of A_i. You have to tell by context alone whether a superscript is the standard power function in arithmetic, or is just a way of labeling an element of a set.

Thus for each $i = 1, \ldots, n$, the elements of A_i can be written as a sequence $a_i^1, a_i^2, a_i^3, \ldots$. Then we can arrange A in a sequence as follows:

$$a_1^1, a_1^2, a_2^1, a_1^3, a_2^2, a_3^1, a_1^4, a_2^3, a_3^1, a_1^4, \ldots.$$

In words, first write down all elements a_i^j of A for which the sum of the subscript and the superscript are 2, then all that sum to three, and so on. Now, if the A_i are not disjoint, drop any instance of a member of A on the list except the first. We now have a denumeration of A—that is, a one-to-one onto mapping with the natural numbers.

This shows that any finite union of denumerable sets is denumerable.

A similar argument shows that the product of denumerable sets $A_1, \ldots, A_n$, $A = A_1 \times A_2 \times \ldots \times A_n$ is itself denumerable. We again choose a denumeration of set A_i so the j^{th} element of A_i is a_i^j. Recall that we can think of elements of A as sequences (ordered n-tuples) of the form $a_1, a_2, \ldots, a_n$ where $a_i \in A_i$ for $i = 1, \ldots, n$. Now write down in some particular order all the sequences whose superscripts add up to n, then $n + 1$, then $n + 2$, and so on. This gives a denumeration of A. By the way, note that I am allowed to leave off the superscript if I don't care about it. If I had put superscripts on $a_1, a_2, \ldots, a_n$ it would look like $a_1^{j_1}, a_2^{j_2}, \ldots, a_n^{j_n}$, which is pretty awful looking.

What if we have a denumerable number of sets $A_1, A_2, \ldots$? It is easy to see that exactly the same methods give denumerations of the union or the product of these sets. To see this, simply go over the above constructions and note that they do not depend on there being a finite number of sets. Therefore the union and product of a denumerable number of denumerable sets is itself denumerable.

Now back to the polynomials with rational coefficients, which we will write as $\mathcal{P}$. Note that by multiplying a polynomial by the product of the denominators of the coefficients, the polynomial then has integer coefficients and exactly the same roots. Thus, we will always assume a polynomial in $\mathcal{P}$ has integer coefficients. There is a natural injection from $\mathcal{P}$ into the denumerable product of the integers, $\mathbb{Z}^\infty = \mathbb{Z} \times \mathbb{Z} \times \ldots$. We start with polynomials of degree one, such as $ax + b$ where $a > 0$. We associate $ax + b$ with $b, a, 0, 0, \ldots$. For a quadratic $ax^2 + bx + c$ we associate $c, b, a, 0, 0, \ldots$. And so on. Now any denumeration of $\mathbb{Z}^\infty$ gives a denumeration of $\mathbf{P}$. But each polynomial in $\mathbf{P}$ has only a finite number of roots, so we can extend the denumeration of $\mathbb{Z}$ that of the algebraic numbers.

Cantor first showed that the algebraic numbers are denumerable, probably using reasoning similar to the above (actually, I don't recall what argument he actually used, if I ever knew it). The true shocker, however, was his extremely simple argument that the reals **R** are *not* denumerable. He did this using the famous *diagonal argument*, which he invented.

Suppose **R** were denumerable, and put all the real numbers between zero and 1 in a list $r_1, r_2, \ldots$. Now let $0.d_i^1 d_i^2, \ldots$ be a decimal representation of r_i, where each of the d_i^j is one of the digits 0,1,2...,9. Such a representation is unique except that a number like 0.1999...can also be written as 0.2. When this occurs, we agree always to use the latter representation. Now create a real number r between zero and one in which the j^{th} digit is $d_j^j + 1$ if $0 \leq d_j^j \leq 7$, 7 if $d_j^j = 8$, 8 if $d_j^j = 9$, and 0 if $d_j^j = 9$. Clearly r cannot be in the list $r_1, r_2, \ldots$ because it differs from each r_i in the i^{th} decimal position. Moreover, r cannot have an expansion ending with $999\ldots$, because there are no 9's in r. Therefore there is no such denumeration of **R**.

Note that this proves that there are *transcendental numbers*, which are numbers that are not the root of any polynomial with integral coefficients. We now know that only a few of the numbers we use in mathematics are actually transcendental numbers, and these include e, the base of the natural logarithms, and π. We do not even know if $e + \pi$ is transcendental or algebraic!

4.12 The Continuum Hypothesis

5

Probability Theory

Doubt is disagreeable, but certainty is ridiculous.

Voltaire

5.1 Introduction

The material you have learned to this point is sufficient to do a surprising amount of real mathematics, including probability theory. We will stick to finite probability spaces because they have none of the weird behavior of infinite probability spaces, and they are arguably much more important and fundamental anyway.

5.2 Probability Spaces

We assume a finite *universe* or *sample space* Ω and a set $\mathcal{X}$ of subsets $A, B, C, \ldots$ of Ω, called *events*. We assume $\mathcal{X}$ is closed under finite unions (if $A_1, A_2, \ldots A_n$ are events, so is $\cup_{i=1}^n A_i$), finite intersections (if $A_1, \ldots, A_n$ are events, so is $\cap_{i=1}^n A_i$), and complementation (if A is an event so is the set of elements of Ω that are not in A, which we write A^c). If A and B are events, we interpret $A \cap B = AB$ as the event "A and B both occur," $A \cup B$ as the event "A or B occurs," and A^c as the event "A does not occur."

For instance, suppose we flip a coin twice, the outcome being HH (heads on both), HT (heads on first and tails on second), TH (tails on first and heads on second), and TT (tails on both). The sample space is then $\Omega = \{HH, TH, HT, TT\}$. Some events are $\{HH, HT\}$ (the coin comes up heads on the first toss), $\{TT\}$ (the coin comes up tails twice), and $\{HH, HT, TH\}$ (the coin comes up heads at least once).

The *probability* of an event $A \in \mathcal{X}$ is a real number $\mathrm{P}[A]$ such that $0 \leq \mathrm{P}[A] \leq 1$. We assume that $\mathrm{P}[\Omega] = 1$, which says that with probability 1 *some* outcome occurs, and we also assume that if $A = \cup_{i=1}^n A_i$, where $A_i \in \mathcal{X}$ and the $\{A_i\}$ are disjoint (that is, $A_i \cap A_j = \emptyset$ for all $i \neq j$), then

$\mathrm{P}[A] = \sum_{i=1}^{n} P[A_i]$, which says that probabilities are additive over finite disjoint unions.[1]

5.3 De Morgan's Laws

Show that for any two events A and B, we have

$$(A \cup B)^c = A^c \cap B^c$$

and

$$(A \cap B)^c = A^c \cup B^c.$$

These are called *De Morgan's laws*. Express the meaning of these formulas in words.

Show that if we write p for proposition "event A occurs" and q for "event B occurs," then

$$\text{not } (p \text{ or } q) \Leftrightarrow (\text{ not } p \text{ and not } q),$$

$$\text{not } (p \text{ and } q) \Leftrightarrow (\text{ not } p \text{ or not } q).$$

The formulas are also De Morgan's laws. Give examples of both rules.

5.4 Interocitors

An interocitor consists of two kramels and three trums. Let A_k be the event "the kth kramel is in working condition," and B_j is the event "the jth trum is in working condition." An interocitor is in working condition if at least one of its kramels and two of its trums are in working condition. Let C be the event "the interocitor is in working condition." Write C in terms of the A_k and the B_j.

5.5 The Direct Evaluation of Probabilities

THEOREM 5.1 *Given $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$, all distinct, there are $n \times m$ distinct ways of choosing one of the a_i and one of the b_j. If we also have $c_1, \ldots, c_r$, distinct from each other, the a_i and the b_j, then there are $n \times m \times r$ distinct ways of choosing one of the a_i, one of the b_j, and one of the c_k.*

[1]The notation $\sum$, which is the Greek letter capital sigma, always means "sum" in formulas. We write $\sum_{i=1}^{n} a_i = a_1 + \ldots + a_n$. Sometimes if it is obvious what the summation is over, we just write $\sum_i a_i$ or even $\sum a_i$.

Apply this theorem to determine how many different elements there are in the sample space of

a. the double coin flip
b. the triple coin flip
c. rolling a pair of dice

Generalize the theorem.

5.6 Probability as Frequency

Suppose the sample space Ω consists of a finite number n of equally probable elements. Suppose the event A contains m of these elements. Then the *probability of the event* A is m/n.

A second definition: Suppose an experiment has n distinct outcomes, all of which are equally likely. Let A be a subset of the outcomes, and $n(A)$ the number of elements of A. We define the *probability* of A as $\mathrm{P}[A] = n(A)/n$.

For example, in throwing a pair of dice, there are $6 \times 6 = 36$ mutually exclusive, equally likely events, each represented by an ordered pair (a, b), where a is the number of spots showing on the first die and b the number on the second. Let A be the event that both dice show the same number of spots. Then $n(A) = 6$ and $\mathrm{P}[A] = 6/36 = 1/6$.

A third definition: Suppose an experiment can be repeated any number of times, each outcome being independent of the ones before and after it. Let A be an event that either does or does not occur for each outcome. Let $n_t(A)$ be the number of times A occurred on all the tries up to and including the t^{th} try. We define the *relative frequency* of A as $n_t(A)/t$, and we define the *probability of* A as

$$\mathrm{P}[A] = \lim_{t \to \infty} \frac{n_t(A)}{t}.$$

We say two events A and B are *independent* if $\mathrm{P}[A]$ does not depend on whether B occurs or not and, conversely, $\mathrm{P}[B]$ does not depend on whether A occurs or not. If events A and B are independent, the probability that both occur is the product of the probabilities that either occurs: that is,

$$\mathrm{P}[A \text{ and } B] = \mathrm{P}[A] \times \mathrm{P}[B].$$

For example, in flipping coins, let A be the event "the first ten flips are heads." Let B be the event "the eleventh flip is heads." Then the two events are independent.

For another example, suppose there are two urns, one containing 100 white balls and 1 red ball, and the other containing 100 red balls and 1 white ball. You do not know which is which. You choose 2 balls from the first urn. Let A be the event "The first ball is white," and let B be the event "The second ball is white." These events are not independent, because if you draw a white ball the first time, you are more likely to be drawing from the urn with 100 white balls than the urn with 1 white ball.

Determine the following probabilities. Assume all coins and dice are "fair" in the sense that H and T are equiprobable for a coin, and $1, \ldots, 6$ are equiprobable for a die.

a. At least one head occurs in a double coin toss.
b. Exactly two tails occur in a triple coin toss.
c. The sum of the two dice equals 7 or 11 in rolling a pair of dice.
d. All six dice show the same number when six dice are thrown.
e. A coin is tossed seven times. The string of outcomes is HHHHHHH.
f. A coin is tossed seven times. The string of outcomes is HTHHTTH.

5.7 Craps

A roller plays against the casino. The roller throws the dice and wins if the sum is 7 or 11, but loses if the sum is 2, 3, or 12. If the sum is any other number (4, 5, 6, 8, 9, or 10), the roller throws the dice repeatedly until either winning by matching the first number rolled or losing if the sum is 2, 7, or 12 ("crapping out"). What is the probability of winning?

5.8 A Marksman Contest

In a head-to-head contest Alice can beat Bonnie with probability p and can beat Carole with probability q. Carole is a better marksman than Bonnie, so $p > q$. To win the contest Alice must win at least two in a row out of three head-to-heads with Bonnie and Carole and cannot play the same person twice in a row (that is, she can play Bonnie-Carole-Bonnie or Carole-Bonnie-Carole). Show that Alice maximizes her probability of winning the contest playing the better marksman, Carole, twice.

5.9 Sampling

The mutually exclusive outcomes of a random action are called *sample points*. The set of sample points is called the *sample space*. An *event A*

is a subset of a sample space Ω. The event A is *certain* if $A = \Omega$ and *impossible* if $A = \emptyset$ (that is, A has no elements). The *probability* of an event A is $\mathrm{P}[A] = n(A)/n(\Omega)$, if we assume Ω is finite and all $\omega \in \Omega$ are equally likely.

a. Suppose six dice are thrown. What is the probability all six die show the same number?
b. Suppose we choose r object in succession from a set of n distinct objects $a_1, \ldots, a_n$, each time recording the choice and returning the object to the set before making the next choice. This gives an ordered sample of the form $(b_1, \ldots, b_r)$, where each b_j is some a_i. We call this *sampling with replacement*. Show that, in sampling r times with replacement from a set of n objects, there are n^r distinct ordered samples.
c. Suppose we choose r objects in succession from a set of n distinct objects $a_1, \ldots, a_n$, without returning the object to the set. This gives an ordered sample of the form $(b_1, \ldots, b_r)$, where each b_j is some unique a_i. We call this *sampling without replacement* . Show that in sampling r times without replacement from a set of n objects, there are

$$n(n-1)\ldots(n-r+1) = \frac{n!}{(n-r)!}$$

distinct ordered samples, where $n! = n \times (n-1) \times \ldots \times 2 \times 1$.

5.10 Aces Up

A deck of 52 cards has 4 aces. A player draws 2 cards randomly from the deck. What is the probability that both are aces?

5.11 Permutations

A linear ordering of a set of n distinct objects is called a *permutation* of the objects. It is easy to see that the number of distinct permutations of $n > 0$ distinct objects is $n! = n \times (n-1) \times \ldots \times 2 \times 1$. Suppose we have a deck of cards numbered from 1 to $n > 1$. Shuffle the cards so their new order is a random permutation of the cards. What is the average number of cards that appear in the "correct" order (that is, the k^{th} card is in the k^{th} position) in the shuffled deck?

5.12 Combinations and Sampling

The number of *combinations* of n distinct objects taken r at a time is the number of subsets of size r, taken from the n things without replacement. We write this as $\binom{n}{r}$. In this case, we do not care about the order of the choices. For instance, consider the set of numbers {1,2,3,4}. The number of samples of size two without replacement = 4!/2! = 12. These are precisely {12,13,14,21,23,24,31,32,34,41,42,43}. The combinations of the four numbers of size two (that is, taken two at a time) are {12,13,14,23,24,34}, or six in number. Note that $6 = \binom{4}{2} = 4!/2!2!$. A set of n elements has $n!/r!(n-r)!$ distinct subsets of size r. Thus, we have

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

5.13 Mechanical Defects

A shipment of seven machines has two defective machines. An inspector checks two machines randomly drawn from the shipment, and accepts the shipment if neither is defective. What is the probability the shipment is accepted?

5.14 Mass Defection

A batch of 100 manufactured items is checked by an inspector, who examines 10 items at random. If none is defective, she accepts the whole batch. What is the probability that a batch containing 10 defective items will be accepted?

5.15 House Rules

Suppose you are playing the following game against the house in Las Vegas. You pick a number between one and six. The house rolls three dice, and pays you $1,000 if your number comes up on one die, $2,000 if your number comes up on two dice, and $3,000 if your number comes up on all three dice. If your number does not show up at all, you pay the house $1,000. At first glance, this looks like a *fair game* (that is, a game in which the expected payoff is zero), but in fact it is not. How much can you expect to win (or lose)?

5.16 The Addition Rule for Probabilities

Let A and B be two events. Then $0 \leq \mathrm{P}[A] \leq 1$ and

$$\mathrm{P}[A \cup B] = \mathrm{P}[A] + \mathrm{P}[B] - \mathrm{P}[AB].$$

If A and B are disjoint (that is, the events are mutually exclusive), then

$$\mathrm{P}[A \cup B] = \mathrm{P}[A] + \mathrm{P}[B].$$

Moreover, if $A_1, \ldots, A_n$ are mutually disjoint, then

$$\mathrm{P}[\cup_i A_i] = \sum_{i=1}^{n} \mathrm{P}[A_i].$$

We call events $A_1, \ldots, A_n$ a *partition* of the sample space Ω if they are mutually disjoint and exhaustive (that is, their union is Ω). In this case for any event B, we have

$$\mathrm{P}[B] = \sum_i \mathrm{P}[BA_i].$$

5.17 A Guessing Game

Each day the call-in program on a local radio station conducts the following game. A number is drawn at random from $\{1, 2, \ldots, n\}$. Callers choose a number randomly and win a prize if correct. Otherwise, the station announces whether the guess was high or low and moves on to the next caller, who chooses randomly from the numbers that can logically be correct, given the previous announcements. What is the expected number $f(n)$ of callers before one guesses the number?

5.18 North Island, South Island

Bob is trying to find a secret treasure buried in the ground somewhere in North Island. According to local custom, if Bob digs and finds the treasure, he can keep it. If the treasure is not at the digging point, though, and Bob happens to hit rock, Bob must go to South Island. On the other hand, if Bob hits clay on North Island, he can stay there and try again. Once on South Island, to get back to North Island, Bob must dig and hit clay. If Bob hits rock on South Island, he forfeits the possibility of obtaining the treasure.

On the other hand, if Bob hits earth on South Island, he can stay on South Island and try again. Suppose q_n is the probability of finding the treasure when digging at a random spot on North Island, r_n is the probability of hitting rock on North Island, r_s is the probability of hitting rock on South Island, and e_s is the probability of hitting earth on South Island. What is the probability, P_n, that Bob will eventually find the treasure before he forfeits, if we assume that he starts on North Island?

5.19 Conditional Probability

If A and B are events, and if the probability $\mathrm{P}[B]$ that B occurs is strictly positive, we define the *conditional probability* of A given B, denoted $\mathrm{P}[A|B]$, by

$$\mathrm{P}[A|B] = \frac{\mathrm{P}[AB]}{\mathrm{P}[B]}.$$

We say $B_1, \ldots, B_n$ are a *partition* of event B if $\cup_i B_i = B$ and $B_i B_j = \emptyset$ for $i \neq j$. We have:

a. If A and B are events, $\mathrm{P}[B] > 0$, and B implies A (that is, $B \subseteq A$), then $\mathrm{P}[A|B] = 1$.
b. If A and B are contradictory (that is, $AB = \emptyset$), then $\mathrm{P}[A|B] = 0$.
c. If $A_1, \ldots, A_n$ are a partition of event A, then

$$\mathrm{P}[A|B] = \sum_{i=1}^{n} \mathrm{P}[A_i|B].$$

d. If $B_1, \ldots, B_n$ are a partition of the sample space Ω, then

$$\mathrm{P}[A] = \sum_{i=1}^{n} \mathrm{P}[A|B_i]\,\mathrm{P}[B_i].$$

5.20 Bayes' Rule

Suppose A and B are events with $\mathrm{P}[A], \mathrm{P}[B], \mathrm{P}[B^c] > 0$. Then we have

$$\mathrm{P}[B|A] = \frac{\mathrm{P}[A|B]\,\mathrm{P}[B]}{\mathrm{P}[A|B]\,\mathrm{P}[B] + \mathrm{P}[A|B^c]\,\mathrm{P}[B^c]}.$$

This follows from the fact that the denominator is just $\mathrm{P}[A]$, and is called *Bayes' rule*.

More generally, if $B_1, \ldots, B_n$ is a partition of the sample space and if $\mathrm{P}[A], \mathrm{P}[B_k] > 0$, then

$$\mathrm{P}[B_k|A] = \frac{\mathrm{P}[A|B_k]\,\mathrm{P}[B_k]}{\sum_{i=1}^{n} \mathrm{P}[A|B_i]\,\mathrm{P}[B_i]}.$$

To see this, note that the denominator on the right-hand side is just $\mathrm{P}[A]$, and the numerator is just $\mathrm{P}[AB_k]$ by definition.

5.21 Extrasensory Perception

Alice claims to have ESP. She says to Bob, "Match me against a series of opponents in picking the high card from a deck with cards numbered 1 to 100. I will do better than chance in either choosing a higher card than my opponent or choosing a higher card on my second try than on my first." Bob reasons that Alice will win on her first try with probability 1/2, and beat her own card with probability 1/2 if she loses on the first round. Thus, Alice should win with probability $(1/2) + (1/2)(1/2) = 3/4$. He finds, to his surprise, that Alice wins about 5/6 of the time. Does Alice have ESP?

5.22 Les Cinq Tiroirs

You are looking for an object in one of five drawers. There is a 20% chance that it is not in any of the drawers, but if it is in a drawer, it is equally likely to be in each one. Show that as you look in the drawers one by one, the probability of finding the object in the next drawer rises if not found so far, but the probability of not finding it at all also rises.

5.23 Drug Testing

Bayes' rule is useful because often we know $\mathrm{P}[A|B]$, $\mathrm{P}[A|B^c]$ and $\mathrm{P}[B]$, and we want to find $\mathrm{P}[B|A]$. For example, suppose 5% of the population uses drugs, and there is a drug test that is 95% accurate: it tests positive on a drug user 95% of the time, and it tests negative on a drug nonuser 95% of the time. Show that if an individual tests positive, the probability of his being a drug user is 50%. Hint: Let A be the event "is a drug user," let "Pos" be the event "tests positive," let "Neg" be the event "tests negative," and apply Bayes' rule.

5.24 Color Blindness

Suppose 5% of men are color-blind and 0.25% of women are color-blind. A person is chosen at random and found to be color-blind. What is the probability the person is male (assume the population is 50% female)?

5.25 Urns

A collection of $n + 1$ urns, numbered from 0 to n, each contains n balls. Urn k contains k red and $n - k$ white balls. An urn is chosen at random and n balls are randomly chosen from it, the ball being replaced each time before another is chosen. Suppose all n balls are found to be red. What is the probability the next ball chosen from the urn will be red? Show that when n is large, this probability is approximately $n/(n + 2)$. Hint: For the last step, approximate the sum by an integral.

5.26 The Monty Hall Game

You are a contestant in a game show. The host says, "Behind one of those three doors is a new automobile, which is your prize should you choose the right door. Nothing is behind the other two doors. You may choose any door." You choose door A. The game host then opens door B and shows you that there is nothing behind it. He then asks, "Now would you like to change your guess to door C, at a cost of $1?" Show that the answer is no if the game show host randomly opened one of the two other doors, but yes if he simply opened a door he knew did not have a car behind it. Generalize to the case where there are n doors with a prize behind one door.

5.27 The Logic of Murder and Abuse

For a given woman, let A be the event "was habitually beaten by her husband" ("abused" for short), let B be the event "was murdered," and let C be the event "was murdered by her husband." Suppose we know the following facts: (a) 5% of women are abused by their husbands; (b) 0.5% of women are murdered; (c) 0.025% of women are murdered by their husbands; (d) 90% of women who are murdered by their husbands had been abused by their husbands; (e) a woman who is murdered but not by her husband is neither more nor less likely to have been abused by her husband than a randomly selected woman.

Nicole is found murdered, and it is ascertained that she was abused by her husband. The defense attorneys for her husband show that the probability that a man who abuses his wife actually kills her is only 4.50%, so there is a strong presumption of innocence for him. The attorneys for the prosecution show that there is in fact a 94.74% chance the husband murdered his wife, independent from any evidence other than that he abused her. Please supply the arguments of the two teams of attorneys. You may assume that the jury was well versed in probability theory, so they had no problem understanding the reasoning.

5.28 The Principle of Insufficient Reason

The principle of insufficient reason says that if you are "completely ignorant" as to which among the states $A_1, \ldots, A_n$ will occur, then you should assign probability $1/n$ to each of the states. The argument in favor of the principle is strong (see Savage 1954 and Sinn 1980 for discussions), but there are some interesting arguments against it. For instance, suppose A_1 itself consists of m mutually exclusive events $A_{11}, \ldots, A_{1m}$. If you are "completely ignorant" concerning which of these occurs, then if $\mathrm{P}[A_1] = 1/n$, we should set $\mathrm{P}[A_{1i}] = 1/mn$. But are we not "completely ignorant" concerning which of $A_{11}, \ldots, A_{1m}, A_2, \ldots, A_n$ occurs? If so, we should set each of these probabilities to $1/(n + m - 1)$. If not, in what sense were we "completely ignorant" concerning the original states $A_1, \ldots, A_n$?

5.29 The Greens and the Blacks

The game of bridge is played with a normal 52-card deck, each of four players being dealt 13 cards at the start of the game. The Greens and the Blacks are playing bridge. After a deal, Mr. Brown, an onlooker, asks Mrs. Black: "Do you have an ace in your hand?" She nods yes. After the next deal, he asks her: "Do you have the ace of spades?" She nods yes again. In which of the two situations is Mrs. Black more likely to have at least one other ace in her hand? Calculate the exact probabilities in the two cases.

5.30 The Brain and Kidney Problem

A mad scientist is showing you around his foul-smelling laboratory. He motions to an opaque, formalin-filled jar. "This jar contains either a brain or a kidney, each with probability 1/2," he exclaims. Searching around

his workbench, he finds a brain and adds it to the jar. He then picks one blob randomly from the jar, and it is a brain. What is the probability the remaining blob is a brain?

5.31 The Value of Eyewitness Testimony

A town has 100 taxis, 85 green taxis owned by the Green Cab Company and 15 blue taxies owned by the Blue Cab Company. On March 1, 1990, Alice was struck by a speeding cab, and the only witness testified that the cab was blue rather than green. Alice sued the Blue Cab Company. The judge instructed the jury and the lawyers at the start of the case that the reliability of a witness must be assumed to be 80% in a case of this sort, and that liability requires that the "preponderance of the evidence," meaning at least a 50% probability, be on the side of the plaintiff.

The lawyer for Alice argued that the Blue Cab Company should pay, because the witness's testimonial gives a probability of 80% that she was struck by a blue taxi. The lawyer for the Blue Cab Company argued as follows. A witness who was shown all the cabs in town would incorrectly identify 20% of the 85 green taxis (that is, 17 of them) as blue, and correctly identify 80% of the 15 blue taxis (that is, 12 of them) as blue. Thus, of the 29 identifications of a taxi as blue, only twelve would be correct and seventeen would be incorrect. Thus, the preponderance of the evidence is in favor of the defendant. Most likely, Alice was hit by a green taxi.

Formulate the second lawyer's argument rigorously in terms of Bayes' rule. Which argument do you think is correct, and if neither is correct, what is a good argument in this case?

5.32 When Weakness Is Strength

Many people have criticized the Darwinian notion of "survival of the fittest" by declaring that the whole thing is a simple tautology: whatever survives is "fit" by definition! Defenders of the notion reply by noting that we can measure fitness (e.g., speed, strength, resistance to disease, aerodynamic stability) independent of survivability, so it becomes an empirical proposition that the fit survive. Indeed, under some conditions it may be simply false, as game theorist Martin Shubik (1954) showed in the following ingenious problem.

Alice, Bob, and Carole are having a shootout. On each round, until only one player remains standing, the current shooter can choose one of the other

players as target and is allowed one shot. At the start of the game, they draw straws to see who goes first, second, and third, and they take turns repeatedly in that order. A player who is hit is eliminated. Alice is a perfect shot, Bob has 80% accuracy, and Carole has 50% accuracy. We assume that players are not required to aim at an opponent and can simply shoot in the air on their turn, if they so desire.

We will show that Carole, the least accurate shooter, is the most likely to survive. As an exercise, you are asked to show that if the player who gets to shoot is picked randomly in each round, then the survivability of the players is perfectly inverse to their accuracy.

There are six possible orders for the three players, each occurring with probability 1/6. We abbreviate Alice as a, Bob as b, and Carole as c, and we write the order of play as xyz, where x,y,z $\in$ {a,b,c}. We let $\pi_i(\text{xyz})$ be the survival probability of player $i \in \{\text{a,b,c}\}$. For instance, $\pi_{\text{a}}(\text{abc})$ is the probability Alice wins when the shooting order is abc. Similarly, if only two remain, let $\pi_i(\text{xy})$ be the probability of survival for player $i =$x,y when only x and y remain, and it is x's turn to shoot.

If Alice goes first, it is clear that her best move is to shoot at Bob, whom she eliminates with probability 1. Then, Carole's best move is to shoot at Alice, whom she eliminates with probability 1/2. If she misses Alice, Alice eliminates Carole. Therefore, we have $\pi_{\text{a}}(\text{abc}) = 1/2$, $\pi_{\text{b}}(\text{abc}) = 0$, $\pi_{\text{c}}(\text{abc}) = 1/2$, $\pi_{\text{a}}(\text{acb}) = 1/2$, $\pi_{\text{b}}(\text{acb}) = 0$, and $\pi_{\text{c}}(\text{acb}) = 1/2$.

Suppose Bob goes first, and the order is bac. If Bob shoots in the air, Alice will then eliminate Bob. If Bob shoots at Carole and eliminates her, Alice will again eliminate Bob. If Bob shoots at Alice and misses, then the order is effectively acb, and we know Alice will eliminate Bob. However, if Bob shoots at Alice and eliminates her, then the game is cb. We have

$$p_{\text{c}}(\text{cb}) = \frac{1}{2} + \frac{1}{2} \times \frac{1}{5} p_{\text{c}}(\text{cb}).$$

The first term on the right is the probability Carole hits Bob and wins straight off, and the second term is the probability that she misses Bob (1/2) times the probability Bob misses her (1/5) times the probability that she eventually wins if it is her turn to shoot. We can solve this equation, getting $p_{\text{c}}(\text{cb}) = 5/9$, so $p_{\text{b}}(\text{cb}) = 4/9$. It follows that Bob will indeed shoot at Alice, so

$$p_{\text{b}}(\text{bac}) = \frac{4}{5} \times \frac{4}{9} = \frac{16}{45}.$$

Similarly, we have $p_{\mathrm{b}}(\mathrm{bca}) = 16/45$. Also,

$$p_{\mathrm{a}}(\mathrm{bac}) = \frac{1}{5}p_{\mathrm{a}}(\mathrm{ca}) = \frac{1}{5} \times \frac{1}{2} = \frac{1}{10},$$

because we clearly have $p_{\mathrm{a}}(\mathrm{ca}) = 1/2$. Similarly, $p_{\mathrm{a}}(\mathrm{bca}) = 1/10$. Finally,

$$p_{\mathrm{c}}(\mathrm{bac}) = \frac{1}{5}p_{\mathrm{c}}(\mathrm{ca}) + \frac{4}{5} \times p_{\mathrm{c}}(\mathrm{cb}) = \frac{1}{5} \times \frac{1}{2} + \frac{4}{5} \times \frac{5}{9} = \frac{49}{90},$$

because $p_{\mathrm{c}}(\mathrm{ca}) = 1/2$. Similarly, $p_{\mathrm{c}}(\mathrm{bca}) = 49/90$. As a check on our work, note that $p_{\mathrm{a}}(\mathrm{bac}) + p_{\mathrm{b}}(\mathrm{bac}) + p_{\mathrm{c}}(\mathrm{bac}) = 1$.

Suppose Carole gets to shoot first. If Carole shoots in the air, her payoff from cab is $p_{\mathrm{c}}(\mathrm{abc}) = 1/2$, and from cba is $p_{\mathrm{c}}(\mathrm{bac}) = 49/90$. These are also her payoffs if she misses her target. However, if she shoots Alice, her payoff is $p_{\mathrm{c}}(\mathrm{bc})$, and if she shoots Bob, her payoff is $p_{\mathrm{c}}(\mathrm{ac}) = 0$. We calculate $p_{\mathrm{c}}(\mathrm{bc})$ as follows.

$$p_{\mathrm{b}}(\mathrm{bc}) = \frac{4}{5} + \frac{1}{5} \times \frac{1}{2}p_{\mathrm{b}}(\mathrm{bc}),$$

where the first term is the probability he shoots Carole (4/5) plus the probability he misses Carole (1/5) times the probability he gets to shoot again (1/2, because Carole misses) times $p_{\mathrm{b}}(\mathrm{bc})$. We solve, getting $p_{\mathrm{b}}(\mathrm{bc}) = 8/9$. Thus, $p_{\mathrm{c}}(\mathrm{bc}) = 1/9$. Clearly, Carole's best payoff is to shoot in the air. Then $p_{\mathrm{c}}(\mathrm{cab}) = 1/2$, $p_{\mathrm{b}}(\mathrm{cab}) = p_{\mathrm{b}}(\mathrm{abc}) = 0$, and $p_{\mathrm{a}}(\mathrm{cab}) = p_{\mathrm{a}}(\mathrm{abc}) = 1/2$. Also, $p_{\mathrm{c}}(\mathrm{cba}) = 49/50$, $p_{\mathrm{b}}(\mathrm{cba}) = p_{\mathrm{b}}(\mathrm{bac}) = 16/45$, and $p_{\mathrm{a}}(\mathrm{cba}) = p_{\mathrm{a}}(\mathrm{bac}) = 1/10$.

The probability that Alice survives is given by

$$\begin{aligned} p_{\mathrm{a}} &= \frac{1}{6}(p_{\mathrm{a}}(\mathrm{abc}) + p_{\mathrm{a}}(\mathrm{acb}) + p_{\mathrm{a}}(\mathrm{bac}) + p_{\mathrm{a}}(\mathrm{bca}) + p_{\mathrm{a}}(\mathrm{cab}) + p_{\mathrm{a}}(\mathrm{cba})) \\ &= \frac{1}{6}\left(\frac{1}{2} + \frac{1}{2} + \frac{1}{10} + \frac{1}{10} + \frac{1}{2} + \frac{1}{10}\right) = \frac{3}{10}. \end{aligned}$$

The probability that Bob survives is given by

$$\begin{aligned} p_{\mathrm{b}} &= \frac{1}{6}(p_{\mathrm{b}}(\mathrm{abc}) + p_{\mathrm{b}}(\mathrm{acb}) + p_{\mathrm{b}}(\mathrm{bac}) + p_{\mathrm{b}}(\mathrm{bca}) + p_{\mathrm{b}}(\mathrm{cab}) + p_{\mathrm{b}}(\mathrm{cba})) \\ &= \frac{1}{6}\left(0 + 0 + \frac{16}{45} + \frac{16}{45} + 0 + \frac{16}{45}\right) = \frac{8}{45}. \end{aligned}$$

The probability that Carole survives is given by

$$p_{\mathrm{C}} = \frac{1}{6}(p_{\mathrm{C}}(\mathrm{abc}) + p_{\mathrm{C}}(\mathrm{acb}) + p_{\mathrm{C}}(\mathrm{bac}) + p_{\mathrm{C}}(\mathrm{bca}) + p_{\mathrm{C}}(\mathrm{cab}) + p_{\mathrm{C}}(\mathrm{cba}))$$
$$= \frac{1}{6}\left(\frac{1}{2} + \frac{1}{2} + \frac{49}{90} + \frac{49}{90} + \frac{1}{2} + \frac{49}{90}\right) = \frac{47}{90}.$$

You can check that these three probabilities add up to unity, as they should. Note that Carole has a 52.2% chance of surviving, whereas Alice has only a 30% chance, and Bob has a 17.8% chance.

5.33 The Uniform Distribution

The *uniform distribution* on $[0, 1]$ is a random variable that is uniformly distributed over the unit interval. Therefore if $\tilde{x}$ is uniformly distributed over $[0, 1]$ then

$$\mathrm{P}[\tilde{x} < x] = \begin{cases} 0 & x \leq 0 \\ x & 0 \leq x \leq 1 \\ 1 & 1 \leq x. \end{cases}$$

If $\tilde{x}$ is uniformly distributed on the interval $[a, b]$, then $(\tilde{x} - a)/(b - a)$ is uniformly distributed on $[0, 1]$, and a little algebra shows that

$$\mathrm{P}[\tilde{x} < x] = \begin{cases} 0 & x \leq a \\ \frac{x-a}{b-a} & a \leq x \leq b \\ 1 & b \leq x. \end{cases}$$

Figure 5.1 depicts this problem.

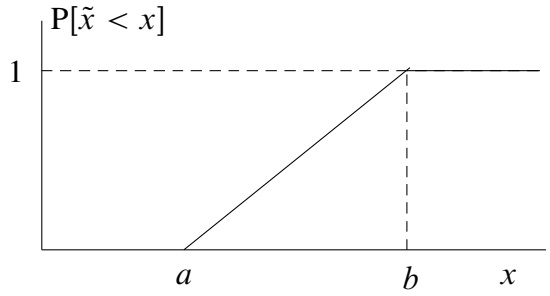

Figure 5.1. Uniform distribution

Suppose $\tilde{x}$ is uniformly distributed on $[a, b]$ and we learn that in fact $\tilde{x} \leq c$, where $a < c < b$. Then $\tilde{x}$ is in fact uniformly distributed on $[a, c]$. To see this, we write

$$\begin{aligned} \mathrm{P}[\tilde{x} < x | \tilde{x} \leq c] &= \frac{\mathrm{P}[\tilde{x} < x \text{ and } \tilde{x} \leq c]}{\mathrm{P}[\tilde{x} \leq c]} \\ &= \frac{\mathrm{P}[\tilde{x} < x \text{ and } \tilde{x} \leq c]}{(c-a)/(b-a)}. \end{aligned}$$

We evaluate the numerator as follows:

$$\begin{aligned} \mathrm{P}[\tilde{x} < x \text{ and } \tilde{x} \leq c] &= \begin{cases} 0 & x \leq a \\ \mathrm{P}[\tilde{x} < x] & a \leq x \leq c \\ \mathrm{P}[\tilde{x} \leq c] & c \leq x \end{cases} \\ &= \begin{cases} 0 & x \leq a \\ \frac{x-a}{b-a} & a \leq x \leq c \\ \frac{c-a}{b-a} & c \leq x \end{cases}. \end{aligned}$$

Therefore,

$$\mathrm{P}[\tilde{x} < x | \tilde{x} \leq c] = \begin{cases} 0 & x \leq 0 \\ \frac{x-a}{c-a} & a \leq x \leq c \\ 1 & c \leq x \end{cases}.$$

This is just the uniform distribution on $[a, c]$.

5.34 Laplace's Law of Succession

An urn contains a large number n of white and black balls, where the number of white balls is uniformly distributed between 0 and n. Suppose you pick out m balls with replacement, and r are white. Show that the probability of picking a white ball on the next draw is approximately $(r+1)/(m+2)$.

5.35 From Uniform to Exponential

Bob tells Alice to draw repeatedly from the uniform distribution on $[0, 1]$ until her current draw is less than some previous draw, and he will pay her $\$n$, where n is the number of draws. What is the average value of this game for Alice?

6

Vector Spaces

6.1 The Origins of Vector Space Theory

The discovery of a way to integrate algebra and plane geometry was among the greatest of the many achievements of the reknown French philosopher René Descartes. Descartes noticed that if you take Euclid's plane geometry and associate an ordered pair of real numbers (x, y) with each *point*, a *line* could be identified with the set of points satisfying the linear equation $ax + by = c$, where $a, b, c \in \mathbf{R}$. He then discovered that a circle could be identified with the solution to the quadratic equation $x^2 + y^2 = r^2$, where $r > 0$ is the radius of the circle. Analytic geometry was born, and with the notion of the plane as a two dimensional space $\mathbf{R}^2$. But the story does not end there, or even with the generalization of a point to an ordered set of n real numbers $(x_1, \ldots, x_n)$, giving rise to n-dimensional real space $\mathbf{R}^n$ for any natural number $n > 0$.

One of Euclid's axioms is that every pair of points uniquely identifies a line. Algebraically we can find this line, given the two points $\mathbf{v}_1 = (x_1, y_1)$ and $\mathbf{v}_2 = (x_2, y_2)$, by solving the pair equations

$$ax_i + by_i = c \qquad i = 1, 2$$

for a, b, and c, getting, as long as $x_1 y_2 \neq x_2 y_1$,

$$a = c\frac{y_2 - y_1}{x_1 y_2 - x_2 y_1}, \qquad b = c\frac{x_2 - x_1}{x_1 y_2 - x_2 y_1}, \tag{6.1}$$

where c is any non-zero real number. If $x_1 y_2 = x_2 y_1$ but $x_1 \neq x_2$, then $c = 0$ and $a/b = (y_2 - y_1)/(x_2 - x_1)$, so the line is through the origin with slope a/b. Finally, if $x_1 = x_2$, then the line is the horizontal line $\{(x, y) | x = x_1\}$.

As you can see, the description of the line between two points is quite inelegant and hard to use because we must discuss three distinct cases. Thus, every time we want to study something using a line, we have to deal with

three separate cases. If we want to talk about k lines, we must deal with 3^k separate cases!

However, you could also note that if we define the product of a real number r and a point $\mathbf{v} = (x, y)$ as $r\mathbf{v} = r(x, y) = (rx, ry)$, and if we define the *addition* of two points as $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, then the line including $\mathbf{v}_1$ and $\mathbf{v}_2$ simply as the set of points

$$\{\mathbf{v}^r = r\mathbf{v}_1 + (1 - r)\mathbf{v}_2 | r \in \mathbf{R}\}. \tag{6.2}$$

To show this, we do have to consider all three cases, but when we are satisfied that this set really is the line between $\mathbf{v}_1$ and $\mathbf{v}_2$, we will never again have to consider special cases. So, suppose $x_1 y_2 \neq x_2 y_1$. Then the formulas (6.1) hold, and if we substitute in any point $(x, y) = r\mathbf{v}_1 + (1-r)\mathbf{v}_2$, you can check that indeed $ax + by = c$, where a and b are given by (6.1), and simplify, we get c. I leave it to the reader to check the cases $x_1 y_2 = x_2 y_1$ but $x_1 \neq x_2$, and $x_1 = x_2$.

It is also true that the line segment between $\mathbf{v}_1$ and $\mathbf{v}_2$ is just the set of points $\{r\mathbf{v}_1 + (1 - r)\mathbf{v}_2 | r \in [0, 1]\}$.[1] Indeed, the point $r\mathbf{v}_1 + (1 - r)\mathbf{v}_2$ divides the line segment between $\mathbf{v}_1$ and $\mathbf{v}_2$ in the ratio $r : 1 - r$, so, for instance, $\mathbf{v}^0 = \mathbf{v}_2$, $\mathbf{v}^1 = \mathbf{v}_1$, $\mathbf{v}^{1/2}$ is the midpoint of the line segment, and so on.

The easiest way to prove these statements is to move one of the points to a position where the calculations are easy, prove the statements there, and then show that the result does not depend on the absolute location of the points, but only on their relative location to each other. In this case, let's move $\mathbf{v}_2$ to the origin, so $\mathbf{v}_2 = \mathbf{0} = (0, 0)$ the so-called *zero vector*. In this case, $\mathbf{v}^r = r\mathbf{v}_1$, for which it is obvious that $\mathbf{v}^r$ is on a line with the same slope as the line through the origin and $\mathbf{v}_1$, so the two lines must be the same. To prove the assertion that $\mathbf{v}^r$ cuts the line segment between $\mathbf{0}$ and $\mathbf{v}_1$ in the ratio $r : 1 - r$, we must define the *distance* between a point and the zero vector $\mathbf{0}$. We define this just as you learned in algebra: the length of the line segment from $\mathbf{0}$ to $\mathbf{v} = (x, y)$ is $|\mathbf{v}| = \sqrt{x^2 + y^2}$. From this definition, you can see that $r|\mathbf{v}| = |r\mathbf{v}|$ if $r \geq 0$. This shows that $\mathbf{v}^r$ divides the line segment between $\mathbf{0}$ and $\mathbf{v}_1$ in the ratio $r : 1 - r$.

[1] Note that $[0, 1]$ means $\{r \in \mathbf{R} | 0 \leq r \leq 1\}$, and is called the *closed interval* between zero and one. We also commonly use $(0, 1)$, the *open interval* between zero and one, to be the closed interval excluding its endpoints, zero and one. Indeed, for arbitrary real numbers $a < b$, we have intervals $[a, b]$, (a, b), and even $[a, b)$ and $(a, b]$, the latter two including one endpoint but not the other. An interval of numbers with exactly one endpoint included is called a *half-open interval*. For instance, $(a, b] = \{r \in \mathbf{R} | a < r \leq b\}$.

Now suppose $\mathbf{v}_2$ is an arbitrary point distinct from $\mathbf{v}_1$. We define the distance between $\mathbf{v}_1$ and $\mathbf{v}_2$ to be $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$, which coincides with our previous definition when $\mathbf{v}_2 = \mathbf{0}$. Moreover, if we define *subtraction* of points in the obvious way as $(x_1, y_1) - (x_2, y_2) = (x_1 - x_2, y_1 - y_2)$, then the distance between $\mathbf{v}_2$ and $\mathbf{v}_1$ is the same as the distance between $\mathbf{0}$ and $\mathbf{v}_1 - \mathbf{v}_2$. Thus all our distance arguments go through with arbitrary $\mathbf{v}_2$ just as they did with $\mathbf{v}_2 = \mathbf{0}$.

6.2 The Vector Space Axioms

We develop the ideas presented above by defining an abstract algebraic structure that generalizes the properties of $\mathbf{R}^n$ for $n \in \mathbb{N}$. A vector space over an arbitrary field $\mathcal{F}$ is a set V, an element of which is called a *vector*, with a special vector $\mathbf{0}$ and the operations *vector addition* $(\mathbf{a}, \mathbf{b} \mapsto \mathbf{a} + \mathbf{b})$, *vector negation* $(\mathbf{a} \mapsto -\mathbf{a}$, and *scalar multiplication* $(r, \mathbf{a} \mapsto r\mathbf{a})$, for any $\mathbf{a}, \mathbf{b} \in V$ and $r \in \mathcal{F}$.

We assume first that V is an commutative group with identity $\mathbf{0}$ under addition. This means that for any $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$, we have

$$\begin{aligned} (\mathbf{a} + \mathbf{b}) + \mathbf{c} &= \mathbf{a} + (\mathbf{b} + \mathbf{c}); \\ 0 + \mathbf{a} &= \mathbf{a} + 0 = \mathbf{a}; \\ (-\mathbf{a}) + \mathbf{a} &= \mathbf{a} + (-\mathbf{a}) = 0. \end{aligned}$$

We abbreviate $\mathbf{a} + (-\mathbf{b})$ as $(\mathbf{a} - \mathbf{b})$, and we call the new operation $\mathbf{a}, \mathbf{b} \mapsto \mathbf{a} - \mathbf{b}$ *vector subtraction*.

We assume second that scalar multiplication satisfies $0\mathbf{a} = \mathbf{0}$, $1\mathbf{a} = \mathbf{a}$, and for any $r, s \in \mathcal{F}$ and any $\mathbf{a} \in V$, $(rs)\mathbf{a} = r(s\mathbf{a})$.

Finally, we assume the same distributive laws that obviously hold in $\mathbf{R}^n$, namely, for $\mathbf{a}, \mathbf{b} \in V$ and $r, s \in \mathcal{F}$, we have

$$\begin{aligned} r(\mathbf{a} + \mathbf{b}) &= r\mathbf{a} + r\mathbf{b} \\ (r + s)\mathbf{a} &= r\mathbf{a} + s\mathbf{a}. \end{aligned}$$

6.3 Norms on Vector Spaces

Suppose the field $\mathcal{F}$ is the real numbers $\mathbf{R}$. An *inner product* on the vector space V is a map $\mathbf{a}, \mathbf{b} \mapsto \mathbf{a} \cdot \mathbf{b}$ with the following properties:

$$\begin{aligned} \mathbf{a} \cdot \mathbf{b} &= \mathbf{b} \cdot \mathbf{a} \\ (r\mathbf{a}) \cdot \mathbf{b} &= r(\mathbf{a} \cdot \mathbf{b}) \\ (r+s) \cdot \mathbf{a} &= r \cdot \mathbf{a} + s \cdot \mathbf{a} \\ \mathbf{a} \cdot \mathbf{a} &\geq \mathbf{0} \\ \mathbf{a} \cdot \mathbf{a} = \mathbf{0} &\rightarrow \mathbf{a} = \mathbf{0}. \end{aligned}$$

If $V = \mathbf{R}^n$, then the most common inner product is given by

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) \cdot = (x_1 y_1, \ldots, x_n y_n).$$

With this inner product, we have $|\mathbf{a}| = \sqrt{\mathbf{a} \cdot \mathbf{a}}$.

6.4 Properties of Norm and Inner Product

Let V be a normed vector space with an inner product over the real number field $\mathbf{R}$. It is easy to show that for any $\mathbf{a} \in V$, $r \in \mathbf{R}$,

$$|r\mathbf{a}| = r|\mathbf{a}|.$$

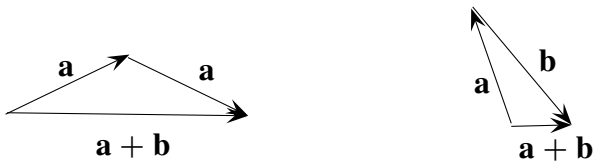

Figure 6.1. The Triangle Inequality

Moreover, the standard *triangle inequality* holds: for $\mathbf{a}, \mathbf{b} \in V$

$$|\mathbf{a} + \mathbf{b}| \leq |\mathbf{a}| + |\mathbf{b}|.$$

The triangle inequality is illustrated in figure 6.1.

The *parallelogram law* says that for $\mathbf{a}, \mathbf{b} \in V$,

$$|\mathbf{a} + \mathbf{b}|^2 + |\mathbf{a} - \mathbf{b}|^2 = 2|\mathbf{a}|^2 + 2|\mathbf{b}|^2$$

To prove this, just multiply out the left hand side, which is

$$(\mathbf{a}+\mathbf{b})\cdot(\mathbf{a}+\mathbf{b})+(\mathbf{a}-\mathbf{b})\cdot(\mathbf{a}-\mathbf{b})$$

using the distributive and other laws of the inner product, and compare with the right hand side.

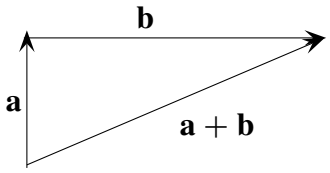

Figure 6.2. The Pythagorean Theorem

We say two vectors **a**, and **b** are *orthogonal* if $\mathbf{a}\cdot\mathbf{b}=0$. The *Pythagorean theorem* says that if **a** and **b** are orthogonal, then

$$|\mathbf{a}|^2+|\mathbf{b}|^2=|\mathbf{a}+\mathbf{b}|^2.$$

This is illustrated in figure 6.2.

More generally, we have

$$|\mathbf{a}|^2+|\mathbf{b}|^2=|\mathbf{a}+\mathbf{b}|^2+2\mathbf{a}\cdot\mathbf{b},$$

which can also easily be proved by multiplying out both sides.

6.5 The Dimension of a Vector Space

In the n-dimensional vector space $\mathbf{R}^n$, we can define n *basis vectors* $\mathbf{e}_1,\ldots,\mathbf{e}_n$, where $\mathbf{e}_i = (0,\ldots,0,1,0\ldots,0)$, where the '1' is in the i^{th} position. It is easy to see that each basis vector has length one, any two distinct basis vectors are orthogonal, and for any vector $\mathbf{v}=(x_1,\ldots,x_n)$, we have a unique expression for **v** in terms of the basis vectors given by

$$\mathbf{v}=\sum_{i=1}^{n}x_i\mathbf{e}_i = x_1\mathbf{e}_1+x_2\mathbf{e}_2+\ldots+x_n\mathbf{e}_n. \tag{6.3}$$

It turns out that this idea of a basis extends to any vector space, and there is a unique number n of basis vectors in any finite dimensional vector space. If you think about this for a minute, you will realize that this means that

there is really a *unique* vector space of dimension n over a field $\mathcal{F}$, in the sense that there is an *isomorphism* between any two vector spaces V_1 and V_2 of dimension n over $\mathcal{F}$. An isomorphism is a bijection that preserves vector addition and scalar multiplication. To define such an isomorphism, which is not unique, choose a basis for each vector space, say $\mathbf{e}_1, \ldots, \mathbf{e}_n$ for V_1 and $\mathbf{f}_1, \ldots, \mathbf{f}_n$ for V_2, let $\phi(\mathbf{e}_i) = \mathbf{f}_i$ for each $i = 1, \ldots, n$, and extend ϕ to all of V_1 by defining, for $\mathbf{v}$ as in (6.3),

$$\phi(\mathbf{v}) = x_1\mathbf{f}_1 + x_2\mathbf{f}_2 + \ldots + x_n\mathbf{f}_n.$$

or more succinctly,

$$\phi\left(\sum_{i=1}^{n} x_i \mathbf{e}_i\right) = \sum_{i=1}^{n} x_i \mathbf{f}_i.$$

The mapping $\phi : V_1 \to V_2$ is the desired isomorphism, as you can easily show.

We say that a set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$ *generates* V, or *spans* V if, for any $\mathbf{v} \in V$, there are k elements $x_i \in \mathcal{F}$ such that $\mathbf{v} = \sum_{i=1}^{k} k_i x_i$. We say V is *finite dimensional* if V has a finite set v of vectors that spans V. We say a set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are *linearly independent* if $x_1\mathbf{v}_1 + \ldots + x_n\mathbf{v}_n = 0$ for $x_1, \ldots, x_n \in \mathcal{F}$, then $x_1 = x_2 = \ldots = x_n = 0$. This means that no vector in the set can be written as a linear combination of the others. Note the when $\mathcal{F} = \mathbf{R}$ and the vectors space is $\mathbf{R}^n$, then the basis vectors $\mathbf{e}_i$ are linearly independent.

We say $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ is a *basis* for V if they span V and are linearly independent. We shall show that if one basis for V has n elements, all bases for V have n elements. We call n the *dimension* of V, and we say V is *finite dimensional*.

We must prove that all bases have the same number of elements. We will also prove that if vector space V has dimension n, then any linearly independent set of n vectors generates V, and hence forms a basis for V. Moreover, any set of linearly independent vectors form part of (i.e., can be extended to) a basis for V.

To prove the above assertions, suppose $v = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $w = \{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ are bases of V. We will show that $k \geq n$, which of course implies $k = n$. Because w spans v, we can write $\mathbf{v}_1$ as a linear combinations of vectors in w:

$$\mathbf{v}_1 = \sum_i x_i \mathbf{w}_i, \qquad x_i \in \mathcal{F}.$$

At least one of the x_i, say x_m, is not zero, so we can rewrite this as

$$\mathbf{w}_m = \frac{1}{x_m}\mathbf{v}_1 - \sum_{i=1, i\neq m}^{k} \frac{x_i}{x_m}\mathbf{v}_i . \tag{6.4}$$

This shows that the set $w_1 = \{\mathbf{v}_1, \mathbf{w}_1, \ldots, \mathbf{w}_k\} - \{\mathbf{w}_m\}$, where we dropped $\mathbf{w}_m$ from w, spans V. Moreover the set w_1 is linearly independent. For if not, then $\mathbf{v}_1$ must be a linear combination of the other vectors in w_1, in which case (6.4) shows that $\mathbf{w}_m$ is a linear combination of the other vectors in w. This contradicts the fact that w is a basis of V. This proves that w_1 is a basis of V. Now, using the same argument, we can add $\mathbf{v}_2$ to w_1 and drop a vector in w from w_1, getting a new basis w_2. It is possible to drop another vector from w because if the coefficients of all the vectors $\mathbf{w}_i$ in w_1 had zero coefficients, then $\mathbf{v}_1$ and $\mathbf{v}_2$ would be linearly dependent, which is false. Continuing in the same way, we end up with a set w_n which, if $k = n$, is simply v, or if $k > n$ is $w_n = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n, \mathbf{w}^{n+1}, \ldots, \mathbf{w}^k\}$, where $\mathbf{w}^{n+1}, \ldots, \mathbf{w}^k \in w$. This shows that $k \geq n$, and since the whole argument can be carried out swapping v and w, this shows that $k = n$.

Now suppose $v = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ are any k linearly independent vectors in V. If $k < n$, then v does not generate V, so there a vector $\mathbf{v}_{k+1}$ that is not generated by v, and hence is linearly independent from v. We can thus add $\mathbf{v}_{k+1}$ to v. We can continue this until v has cardinality n, when which v is a basis for V.

This proof was a little long-winded, but essentially simple, using no sophisticated theorems or properties of vector spaces. Moreover, it is an absolutely fundamental theorem, and is used frequently in mathematical arguments.

6.6 Vector Subspaces

Suppose V is a vector space of dimension $n > 1$, and let $v = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a set of linearly independent vectors in V. From the preceding section, we know that $k \leq n$. Suppose $k < n$. Then it should be clear that the set of vectors spanned by v, call it V_v, is a subset of V that forms a vector space in its own right. this is because $\mathbf{0} \in V_v$, $-v \in V_v$ if $v \in V_v$, and adding vectors in V_v, as well as multiplying vectors in V_v by scalars, always leads to another vector in V_v. We call V_v a *subspace* of V. We say that the dimension of the subspace is k. As an exercise, you might try showing

that if V_v is a subspace of V of dimension k, then any set of k linearly independent vectors in V_v are a basis for V_v, and there are no sets of size larger than k vectors from V_v that are linearly independent.

For instance, in $\mathbf{R}^2$, any line through the origin $(0, 0)$ is a subspace, and in $\mathbf{R}^3$, any plane through the origin, as well as any line through the origin, is a subspace. In $\mathbf{R}^n$, the $n-1$-dimensional subspaces are called *hyperplanes*. Thus, the hyperplanes in $\mathbf{R}^2$ are the lines through the origin, and the hyperplanes in $\mathbf{R}^3$ are the planes through the origin.

6.7 Revisiting the Algebraic Numbers

In section 4.8, we defined an algebraic number as the root of a polynomial equation $a_n x^n + \ldots + a_1 x + a_0$ with rational coefficients, or equivalently, integer coefficients. In section 4.11 We showed that the algebraic numbers are denumerable, and since the complex numbers are non-denumerable, we concluded that not all numbers are algebraic.

With the help of our vector space results, we can say a lot more about algebraic numbers. Let $\mathcal{P}$ be the polynomials with coefficients in the field $\mathbb{Q}$, which is a subfield of the field $\mathcal{C}$ of complex numbers. We know from Theorem 4.1 that every $p \in \mathcal{P}$ has all of its roots in $\mathcal{C}$. Let $a \in \mathcal{C}$ be non-rational, and consider the set of numbers $\mathbb{Q}[a]$ of the form, for any natural number $n > 0$,

$$a_n a^n + \ldots + a_1 a + a_0, \tag{6.5}$$

where $a_n, \ldots, a_0 \in \mathbb{Q}$. It is easy to see that this is a vector space, where addition and scalar multiplication are as defined in $\mathcal{C}$. We write this vector space as $\mathbb{Q}[a]$. If a is algebraic, then this vectors space will be spanned by the vectors $a, a^2, \ldots, a^{n-1}$ and no smaller set of vectors, assuming the polynomial of least degree of which a is a root is of degree n. To see this, note that if this polynomial is $p(x) = a_n x^n + \ldots + a_1 x + a_0$, then $p(a) = 0$ can be rewritten as

$$a^n = -\frac{a_{n-1}}{a_n} a^{n-1} - \ldots - \frac{a_1}{a_n} a - \frac{a_0}{a_n}. \tag{6.6}$$

We could then write a^m for any $m > n-1$ in terms of $a, a^2, \ldots, a^{n-1}$ using (6.6). For instance, multiplying both sides of (6.6) by a, we get

$$a^{n+1} = -\frac{a_{n-1}}{a_n} a^n - \ldots - \frac{a_1}{a_n} a^2 - \frac{a_0}{a_n} a.$$

Now substitute the right hand side of (6.6) for a^6 in the above and simplify. This is complicated, but it simplifies to

$$a^{n+1} = \left(\frac{a_{n-1}^2}{a_n^2} - \frac{a_{n-2}}{a_n}\right)a^{n-1} + \left(\frac{a_{n-1}a_{n-2}}{a_n^2} - \frac{a_{n-3}}{a_n}\right)a^{n-2} + \ldots + \left(\frac{a_{n-1}a_1}{a_n^2} - \frac{a_0}{a_n}\right)a + \frac{a_{n-1}a_0}{a_n^2}.$$

This shows that a^{n+1} can be expressed as a linear combination of the basis vectors $\{1, a, a^2, \ldots, a^{n-1}\}$. Clearly we can extend this calculation to all higher powers of a.

This proves that if a is algebraic but not rational, then $\mathbb{Q}[a]$ is an n-dimensional vector space, where n is the degree of the lowest-degree polynomial of which a is a root. Conversely, if $\mathbb{Q}[a]$ is a finite dimensional vector space, then a must be algebraic, and the dimension of $\mathbb{Q}[a]$ is the degree of the *minimal polynomial* of a.

We can also show that if a is algebraic, then $\mathbb{Q}[a]$ is in fact a field. To show this, we need only show that

$$\frac{q}{a} = a_{n-1}a^{n-1} + \ldots + a_1 a + a_0$$

where q and the coefficients $a_{n-1}, \ldots, a_1, a_0$ lie in $\mathbb{Q}$. To show this, multiply both sides by a, getting the equation

$$a_{n-1}a^n + \ldots + a_1 a^2 + a_0 a - q = 0$$

Because $\mathbb{Q}[a]$ is n-dimension, the vectors $1, a, a^2, \ldots, a^n$ are linearly dependent, so the above equation must have a solution.

A similar argument shows that if $a^1, \ldots, a^k$ are any k algebraic numbers over $\mathbb{Q}$, the vector space $\mathbb{Q}[a^1, \ldots, a^k]$ is finite dimensional, and indeed is a field. Generalizing, the set of all algebraic numbers over $\mathbb{Q}$, which we write $\mathbb{A}$, forms a field. To see this, note that the field axioms can be easily verified for all finite subfields of $\mathbb{A}$, and hence the hold for $\mathbb{A}$.

We may use this type of argument to show that $\mathbb{A}$ is actually *algebraically closed*. That is, any polynomical with coefficients in $\mathbb{A}$ has all of its roots in $\mathbb{A}$. To see this, suppose the polynomial is $p(x) = a_n x^n + \ldots + a_1 x + a_0$ where all coefficients are in $\mathbb{A}$. Consider the vector space $\mathbb{Q}[a_n, \ldots, a_1, a_0]$. We know that this is finite dimensional, spanned by the rational coefficients of the polynomials for which $a_n, \ldots, a_0$ are the roots. But then

$p(a) = 0$ means that $a \in \mathbb{Q}[a_n, \ldots, a_1, a_0]$, so $\mathbb{Q}[a]$ is a vector subspace of $\mathbb{Q}[a_n, \ldots, a_1, a_0]$, and since $\mathbb{Q}[a_n, \ldots, a_1, a_0]$ is finite dimensional, $\mathbb{Q}[a]$ is also finite dimensional, which means that a is algebraic over $\mathbb{Q}$.

7

Real Analysis

7.1 Limits of Sequences

Suppose we have an infinite sequence $a_1, a_2, \ldots$ of real numbers. We write $\lim_{n\to\infty} a_i = a$ if, for every real number $\delta > 0$, there is a natural number n_δ such that the distance between a_i and a is less than δ for all $i > n_\delta$; in symbols,

$$(\forall \delta > 0)(\exists n_\delta \in \mathbb{N})(\forall i > n_\delta)(|a_i - a| < \delta).$$

We say the sequence has *limit* a.

So, for instance, the sequence

$$1, 1/2, 1/3, 1/4, \ldots$$

has limit zero, as you can easily show (given δ, choose n_δ to be any natural number greater than $1/\delta$). For another example, let $k(n)$ be the nearest integer to $n \cdot \sqrt(2)$, and form the sequence

$$k(1)/1, k(2)/2, \ldots, k(n)/n, \ldots. \tag{7.1}$$

You can try you hand a showing that $\lim_{n\to\infty} k(n)/n = \sqrt{2}$.

We write $\lim_{n\to\infty} a_i = \infty$ if, for every real number $d > 0$, there is a natural number n_d such that $a_i > d$ for all $i > n_d$. Note that we could have used δ instead of d as in the previous definition, but by custom, in analysis the Greek letters δ and ϵ are reserved for "very small" real quantities.

Suppose we have an infinite sequence $a_1, a_2, \ldots$ of real numbers such that for every real number $\delta > 0$, there is a natural number n_δ such that the distance between a_i and a_j is less than δ for all $i, j > n_\delta$; in symbols,

$$(\forall \delta > 0)(\exists n_\delta \in \mathbb{N})(\forall i, j > n_\delta)(|a_i - a_j| < \delta).$$

We say the sequence *converges*. Such sequences are called *Cauchy sequences*, named after the French mathematician Augustin Louis Cauchy (1789-1857), the architect of the modern approach to limits, infinitesimals,

and the like. If we are working with the rational number $\mathbb{Q}$, a sequence can converge without converging to anything! A perfectly good example of this is the sequence (7.1), which converges, but not to a rational number (see §4.8). However, the real numbers are *complete*, as defined in 4.10. We will show that every Cauchy sequence converges to a real number.

THEOREM 7.1 Triangle Inequality*: For any real numbers r and s,*

$$|r + s| \leq |r| + |s|.$$

Note that this is just like the triangle inequality for vector spaces (§6.4), and indeed, you can check that $\mathbf{R}$ *is a vector space over itself—a one-dimensional vector space* $\mathbf{R}^1$.
Proof: The theorem is clearly true, and in fact becomes an equality, if r and s have the same sign or at least one is 0. If $r > 0$ *and* $s < 0$*, but* $r + s > 0$*, then* $|r + s| = r + s < r = |r|$*, and similarly if* $s > 0$ *and* $r < 0$ *but* $r + s > 0$*. If* $r > 0$ *and* $s < 0$*, but* $r + s < 0$*, then* $|r + s| = -s - r < -s = |s|$*, and similarly if* $s > 0$ *and* $r < 0$ *but* $r + s < 0$.

THEOREM 7.2 *A sequence of real numbers* $s = a_1, a_2, \ldots$ *converges if and only if there is a real number a such that* $\lim_{n\to\infty} a_i = a$.

Proof: Suppose first that s converges to a, and for a given $\delta > 0$, choose n such that $|a_i - a| < \delta/2$. Then by the triangle inequality,

$$|a_i - a_j| = |(a_i - a) + (a - a_i)| \leq |a_i - a| + |a - a_i| \leq \delta/2 + \delta/2 = \delta.$$

for $i, j > n$. This shows that s is Cauchy.
Now suppose s is Cauchy. It is easy to show that s has an upper bound u. Now each subsequence $s_k = a_k, a_{k+1}, \ldots$ of s is Cauchy and has upper bound u. Then, by completeness of the real numbers, each s_k has a least upper bound b_k. Moreover, the sequence $t = b_1, b_2, \ldots$ is increasing; i.e., $i > j$ implies $b_i \geq b_j$, because b_i is an upper bound to $a_j, \ldots$, but not necessarily a least upper bound. Now the set $\{b_i | i = 1, 2, \ldots\}$ has an upper bound u, so it has a least upper bound a. We show $\lim_{n\to\infty} a_n = a$.
For $\delta > 0$, note that $a - \delta$ is not an upper bound of t, and hence there is an n such that $b_n > a - \delta$. But then $a \geq b_j > a - \delta$ all for $j \geq n$. This implies $|b_j - a| < \delta$ for all $j \geq n$. This shows that t is a Cauchy sequence that converges to a. Now given $\delta > 0$, choose n so that $|b_j - a| < \delta/4$

for $j \geq n$, and choose $m \geq n$ such that $a_m > b_n - \delta/4$. Then we have $|a_m - a| = |(a_m - b_m) + (b_m - a)| \leq |a_m - b_m| + |b_m - a| \leq \delta/2$. Now chose $k \geq m$ such that $|a_m - a_j| < \delta/2$ for $j \geq k$. Then for $j \geq k$, $|a_j - a| = |a_j - a_m + a_m - a| \leq |a_j - a_m| + a_m - a| \leq \delta$. This finishes the proof.

7.2 Compactness and Continuity in R

THEOREM 7.3 Local Compactness of the Real Numbers*: Let* $I = \{[a_i, b_i] \subset \mathbf{R} | a \leq a_i, b_i \leq b, i = 1, 2 \ldots\}$ *be a set of bounded closed intervals such that* $[a_i, b_i] \subseteq [a_j, b_j]$ *for* $i < j$*. Then* I *has a non-empty intersection; i.e., there is a* $c \in \mathbf{R}$ *such that* $c \in [a_i, b_i]$ *for* $i = 1, 2, \ldots$.

Proof: The sequence $b_1, b_2, \ldots$ is decreasing and has a as a lower bound, so the sequence has a greatest lower bound b_*. Similarly, the sequence $a_1, a_2, \ldots$ is increasing, bounded above by b, and so has a least upper bound a^*. Because each b_i is an upper bound of $a_1, a_2, \ldots$, each $b_i \geq a^*$, and therefore a^* is a lower bound of $b_1, b_2, \ldots$, so because b_* is the greatest lower bound of $b_1, b_2, \ldots$, we have $b_* \geq a^*$. The interval $[a^*, b_*]$ (which may be a single point if $a^* = b_*$) is included in all the intervals in I, because each $a_i \geq a^*$ and each $b_i \geq b_*$.

We say a function $f : \mathbf{R} \to \mathbf{R}$ is *continuous* at a point $a \in \mathbf{R}$ if, for any sequence $\{a_i | i = 1, \ldots\}$ such that $\lim_{i \to \infty} a_i = a$, we have $\lim_{i \to \infty} f(a_i) = f(a)$. We sometimes write the same thing as $\lim_{x \to a} f(x) = f(a)$. An alternative way to define continuity at a is that for every $\epsilon > 0$ there is a $\delta > 0$ such that $|f(x) - f(a)| < \epsilon$ for all x such that $|x - a| < \epsilon$. In other words, $f(x)$ stays near $f(a)$ when x stays near a.

We have the following theorem.

THEOREM 7.4 *Suppose* $f, g : \mathbf{R} \to \mathbf{R}$*, and* $b, c \in \mathbf{R}$.

a. if f *and* g *are continuous at* $a \in \mathbf{R}$*, then* $af(x) + bg(x)$ *and* $af(x)g(x)$ *are continuous at* a*;*
b. if f *and* g *are continuous at* $a \in \mathbf{R}$ *and if* $g(a) \neq 0$*, then* $f(x)/g(x)$ *is continuous at* a*;*
c. the constant function $f(x) = r$ *is continuous everywhere;*
d. the linear function $f(x) = x$ *is continuous everywhere;*
e. a polynomial function is continuous everywhere;
f. a rational function, meaning a quotient of polynomials, is continuous except perhaps at a root of the denominator.

Sometimes we can take a function that is not continuous at a point and redefine some of its values in a natural way so that it becomes continuous. For instance $f(x) = (x^2 - 1)/(x - 1)$ is undefined at $x = 1$, but we can define it there to be $f(1) = 2$, and it is easy to show that $f(x)$ is now continuous. This is because $(x^2-1)/(x-1) = x+1$ except where $x = 1$.

Recall that $[a, b]$ for $a, b \in \mathbf{R}$ is the closed interval $\{c | a \leq c \leq b\}$. We have

THEOREM 7.5 Intermediate Value Theorem*: Suppose $f(x)$ is continuous at all points on the interval $[a, b]$, and let $r \in [f(a), f(b)]$. then there is some $c \in [a, b]$ such that $f(c) = r$.*

This theorem implies that the image of a closed and bounded interval by a continuous function is an interval.

Proof: Because $r \in [f(a), f(b)]$, we must have $f(a) \leq f(b)$, and if $f(a) = f(b)$, then $f(a) = r$, so the assertion is true. We may thus assume that $f(a) < r < f(b)$. Let c be the least upper bound of the set $A = \{x \in [a, b] | f(x) \leq r\}$. We use the completeness of the real numbers (§4.10) to ensure that c exists. We will show that $f(c) = r$. Suppose that this is false and $f(c) > r$. Then choose $\delta > 0$ such that $|x - c| < \delta$ implies $|f(c) - f(x)| < f(c) - r$ (i.e., choose $\epsilon = f(c) - r > 0$ in the definition of continuity of $f(x)$ at c). But then $f(x) > r$ for $x \in (c - \delta, c + \delta)$, so $c - \delta$ is an upper bound for A, which is a contradiction. So suppose instead that $f(c) < r$. Then choose $\delta > 0$ such that $|x - c| < \delta$ implies $|f(c) - f(x)| < r - f(c)$ (i.e., choose $\epsilon = r - f(c) > 0$). But then $f(x) < r$ for $x \in (c-\delta, c+\delta)$, so $c+\delta$ is an upper bound for A, which is a contradiction. This completes the proof of the Intermediate Value Theorem.

THEOREM 7.6 Bolzano-Weierstrass Theorem*: Let $s = a_1, a_2, \ldots$ be a sequence of real numbers in the interval $[a, b]$. Then there is a number $c \in [a, b]$ and a subsequence $a_{i_1}, a_{i_2}, \ldots$ of s (meaning $i_1 < i_2 < \ldots$) that converges to c.*

Note that c need not be unique; indeed, it could be all of $[a, b]$, as would be the case if s were an enumeration of the rationals in $[a, b]$ (see §3.11).

Proof: Let b_k be the least upper bound of $s_k = a_k, a_{k+1}, \ldots$. Then $b_k \in [a, b]$, and $b_1, b_2, \ldots$ is a weakly increasing sequence (meaning that it cannot decrease, but does not necessarily always increase). Let b be the least upper bound of this sequence. Then $\lim_{k\to\infty} b_k = b$. To see this, choose $\delta > 0$. Then there is an n such that $b_n > b - \delta$, which means that

$b_m > b - \delta$ for all $m \geq n$. This shows that $\lim_{k\to\infty} b_k = b$, which proves the theorem.

The Intermediate Value Theorem shows that the image of a continuous function on an interval $[a, b]$ is an interval (i.e., if it contains two numbers r and s, it contains all the numbers between r and s), but this interval could be unbounded. In fact, it is not. To see this, suppose for each positive integer n there is an $x_n \in [a, b]$ such that $f(x_n) > n$. Then the sequence $s = x_1, x_2, \ldots$ must have a subsequence $t = y_1, y_2, \ldots$ that converges to some number $y \in [a, b]$. But $f(y) = \lim_{k\to\infty} f(y_i)$ because $f(x)$ is continuous, and each $f(y_i) > i$, so $f(y) = \infty$, which is impossible.

This shows that the image of a bounded interval $[a, b]$ by a continuous function is bounded. If r is the least upper bound of this image, then we can show that $r = f(c)$ for some $c \in [a, b]$. A precisely parallel argument shows that the image of $[a, b]$ is bounded from below, and hence has a greatest lower bound w, and in fact $f(d) = w$ for some $d \in [a, b]$. This shows that the image of $[a, b]$ is a closed and bounded interval $[f(d), f(c)]$, where $f(x)$ attains it minimum at d and its maximum at c. To show all of this, we need only prove the so-called Extreme Value Theorem.

THEOREM 7.7 *If $f(x)$ is continuous on a closed interval $[a, b]$, then $f(x)$ achieves both its minimum and its maximum for values of x in $[a, b]$.*

Proof: Let r be the least upper bound of $\{f(x) | x \in [a, b]\}$. For any positive integer n, choose $x_n \in [a, b]$ such that $r - 1/n < f(x_n) < r$. Therefore $\lim_{i\to\infty} f(x_i) = r$. By the Bolzano-Weierstrass Theorem (§7.6), we can assume $\lim_{i\to\infty} x_i = x \in [a, b]$. But then by the continuity of $f(x)$, $r = \lim_{i\to\infty} f(x_i) = f(x)$. This proves $f(x)$ attains it maximum at $x \in [a, b]$. The second half of the theorem is proved in a similar manner.

8

Table of Symbols

$\{a, b, x\}$	Set with members a, b and x
$\{x \mid p(x)\}$	The set of x for which $p(x)$ is true
$p \wedge q$, $p \vee q$,$\neg p$	p and q, p or q, not p
iff	If and only if
$p \Rightarrow q$	p implies q
$p \Leftrightarrow q$	p if and only if q
(a, b)	Ordered pair: $(a, b) = (c, d)$ iff $a = c$ and $b = d$
$a \in A$	a is a member of the set A
$A \times B$	$\{(a, b) \mid a \in A$ and $b \in B\}$
$\mathbf{R}$	The real numbers
$\mathbf{R}^n$	The n-dimensional real vector space
$(x_1, \ldots, x_n) \in \mathbf{R}^n$	An n-dimensional vector
$f : A \rightarrow B$	A function $b = f(a)$, where $a \in A$ and $b \in B$
$f(\cdot)$	A function f where we suppress its argument
$f^{-1}(y)$	The inverse of function $y = f(x)$
$\sum_{x=a}^{b} f(x)$	$f(a) + \cdots + f(b)$
$S_1 \times \cdots \times S_n$	$\{(s_1, \ldots s_n) \mid s_i \in S_i, i = 1, \ldots n\}$
$\prod_{i=1}^{n} S_i$	$S_1 \times \cdots \times S_n$
ΔS	Set of probability distributions (lotteries) over S
$\Delta^* \prod_i S_i$	$\Pi_i \Delta S_i$ (set of mixed strategies)
$[a, b]$,(a, b)	$\{x \in \mathbf{R} \mid a \leq x \leq b\}$,$\{x \in \mathbf{R} \mid a < x < b\}$
$[a, b)$,$(a, b]$	$\{x \in \mathbf{R} \mid a \leq x < b\}$,$\{x \in \mathbf{R} \mid a < x \leq b\}$
$A \cup B$	$\{x \mid x \in A$ or $x \in B\}$
$A \cap B$	$\{x \mid x \in A$ and $x \in B\}$
$\cup_\alpha A_\alpha$	$\{x \mid x \in A_\alpha$ for some $\alpha\}$
$\cap_\alpha A_\alpha$	$\{x \mid x \in A_\alpha$ for all $\alpha\}$
$A \subset B$	$A \neq B \wedge (x \in A \Rightarrow x \in B)$
$A \subseteq B$	$x \in A \Rightarrow x \in B$
$=_{\text{def}}$	Equal by definition
$[\psi]$	$\{\omega \in \Omega \mid \psi(\omega)$ is true$\}$
$f \circ g(x)$	$f(g(x))$

References

Kahn, Peter, "Constructing the Real Numbers," 2007. www.math.cornell.edu/~kahn/naturalnumbers07.pdf.

Mileti, Joseph R., "An Introduction to Axiomatic Set Theory," 2007. www.math.uchicago.edu/~~mileti/teaching/math278/settheory.pdf.

Savage, Leonard J., *The Foundations of Statistics* (New York: John Wiley & Sons, 1954).

Shubik, Martin, "Does the Fittest Necessarily Survive?," in Martin Shubik (ed.) *Readings in Game Theory and Political Behavior* (New York: Doubleday, 1954) pp. 43–46.

Sinn, Hans-Werner, "A Rehabilitation of the Principle of Insufficient Reason," *Quarterly Journal of Economics* 94,3 (May 1980):493–506.