Pure Mathematics for Engineers and Scientists

Anthony Daniell

May 16, 2025

Preface

The basic aim is to provide exposure to a solid foundation of mathematics based on proofs. The exit goals would be:

-Readers will be able to write valid proofs using the standard techniques of modern mathematics.

-Readers will be able to read and understand proofs at some reasonable level.

-Readers will have working knowledge of broad foundations of mathematics, and be able to confidently take dedicated courses in each area, or pursue independent studies.

From my experience, I certainly never got this stuff explicitly, but on retrospect, it certainly seems like it would help.

My original concept was that the course would be targeted from someone maybe at the junior or senior level in physics/engineering. So, the typical prerequisite would be calculus, maybe differential equations, and experience applying this math to physics, engineering problems like in mechanics, electricity and magnetism, etc. That's essentially my background, so that's why I thought of this cohort.

The main reason is that this person, in my concept, would have some context and exposure to different math, and may be better motivated to wanting to understand the underpinnings. Also, they may be more interested to branch out into the other topics on the list as these will likely be important as they take more advanced classes in their careers.

However, that being said, I think the main prerequisite is being interested in pure mathematics, perhaps with some future application in mind, but not necessarily.

Topics to be covered:

Mathematical Foundations - Mathematical logic, basic notation, axiomatic set theory (Zermelo-Fraenkel), Peano Axioms of Arithmetic, Gödel theorems.

Methods of Proof: Induction, Contradiction, Direct Proofs. Examples of classic proofs - infinite primes, irrationality of square root of two, etc. Plenty of practice examples.

Real Analysis - Study of real numbers, including construction by Dedekind Cuts etc, point set topology, continuity, metric spaces (Basically a compressed version of Rudin or equivalent).

Modern Algebra: Groups, Rings, Fields, Transformations, Representation Theory, Modules, Galois Theory

Non-euclidean geometry and topology: Various spaces and properties. Invariants, knot theory, homotopy, homology.

Number theory:

Category theory:

Computational complexity theory: Finite Automata, lambda calculus, NP and other spaces.

Contents

Chapter 1

Mathematical Foundations

The objective of this chapter is to present some basic concepts that underlie much of the remaining material in this book.

1.1 Basic Notation

The reader may be familiar with some if not all of the following notation, but it is presented here for concreteness and review.

- $\forall$ is read as "for all"
- $\exists$ is read as "exists"
- $\subset$ is read as "subset of"
- $\in$ is read as "in"
- $\mathbb{Z}$ is the set of integers: $\ldots, -2, -1, 0, 1, 2, 3, \ldots$
- $\mathbb{N}$ is the set of natural numbers: $0, 1, 2, 3, \ldots$ (note: Sometimes these start with 0, and sometimes with 1. Usually doesn't matter to the argument in question, but the reader should be aware.)
- $\mathbb{Q}$ is the set of rational numbers. These are numbers of the form $\frac{p}{q}$ where p, q are integers, and $q \neq 0$
- $\mathbb{R}$ is the set of real numbers. These will later be defined precisely in terms of *Dedekind Cuts*, but for now we'll just use the informal notion of all the points on a coordinate line. However, hopefully the reader can see this is not good enough for precise work.
- We use curly braces to indicate sets in general. For example, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3 \ldots\}$ defines the set of integers using the curly braces and examples. It is hoped the reader is able to abstract that the dots to the left imply the list has

no smallest negative value and the dots to the right imply that there is no largest positive value.

- Set builder notation: There are other ways to specify the set within the braces. For example, we can indicate the property that each member of the set has: $S = \{p | p = 2m + 1, m \in \mathbb{Z}\}$. This is read as the set S consists of those values p of the form $2m+1$ where m is an integer. In other words, S the set of odd integers. The vertical bar in the braces is read as "such that" and the comma is read as "and."

Exercise
Write the definition of the set of rational numbers using set builder notation.
Solution
$\mathbb{Q} = \left\{ r | r = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0 \right\}$

1.2 Mathematical Logic

It should be remarked that a good portion of this section (as well as some others) was strongly inspired by the YouTube video series "Math Major Basics" by MathDoctorBob (https://www.youtube.com/playlist?list=PLF2DF6C3C8015DF5F). We cover some key aspects here. It is very helpful to understand *Truth Tables* in this context. For those who have some experience with digital logic or computer programming, much of this will be quite familiar.

We have the following logical relations, with symbols, defined by the truth tables shown below: Negation ($\neg$), Conjunction/And ($\wedge$ - note that this symbol looks like the outline of the letter "A", to help you remember "And"), Disjunction/or ($\vee$), Implication ($\Longrightarrow$), If and Only If ($\Longleftrightarrow$):

Negation:

A	$\neg A$
T	F
F	T

Conjunction/And:

A	$\wedge$	B
T	T	T
T	F	F
F	F	T
F	F	F

Disjunction/Or:

A	$\vee$	B
T	T	T
T	T	F
F	T	T
F	F	F

Implication:

A	$\Longrightarrow$	B
T	T	T
T	F	F
F	T	T
F	T	F

If and only if (Iff):

A	$\Longleftrightarrow$	B
T	T	T
T	F	F
F	F	T
F	T	F

In the above, A and B are statements which can be either true (T) or false (F). The result of the logical operation is shown in the column under the particular symbol. For example, if A is true, and B is true, then $A \wedge B$ is true. However, either either A or B is false (or both) then $A \wedge B$ is false. It is important to refer back to the truth table definitions of these logical operations to avoid confusion.

Sometimes, implication is called "if-then" as in "If A then B." However, note that it is possible for A to be false and B to be true, and the implication $A \Longrightarrow B$ to be true. This is somewhat at odds with how this if-then might be expressed in common usage: How could something false imply something true? This seems confusing. Therefore, always refer to the truth table for clarity on this point.

Here is an illustration regarding implication ($\Longrightarrow$).

Let $A = (a > 5), B = (a > 3)$ where a is some integer. Now consider the following cases:
If $a = 6, (6 > 5) = T, (6 > 3) = T$
If $a = 4, (4 > 5) = F, (4 > 3) = T$
If $a = 2, (2 > 5) = F, (2 > 3) = F$

If we compare this to the truth table for implication, we see that implication is always true. Note that with this particular definition of the statements A and B we cannot have a case where A is true and B is false.

Exercise Show $A \Longleftrightarrow B$ is equivalent to $(A \Longrightarrow B) \wedge (B \Longrightarrow A)$.

Solution

$(A$	$\Longrightarrow$	$B)$	$\wedge$	$(B$	$\Longrightarrow$	$A)$
T	T	T	T	T	T	T
T	F	F	F	F	T	T
F	T	T	F	T	F	F
F	T	F	T	F	T	F

We now consider some important terminology:

- *Tautology*: Any statement that is true for all values of its components is a tautology.
- *Contradiction*: Any statement that is false for all values of its components is a contradiction. The negation of a contradiction is a tautology and the negation of a tautology is a contradiction.
- *Logically Equivalent*: When $A \Longleftrightarrow B$ is a tautology. This means A and B have the same truth table. The notation for this is $A \equiv B$.

We illustrate logical equivalence by considering "De Morgan's Laws" for disjunction (or) and conjunction (and). De Morgan's Law's are useful for manipulating logical expressions:

$\neg (A \vee B) \equiv (\neg A) \wedge (\neg B)$
$\neg (A \wedge B) \equiv (\neg A) \vee (\neg B)$

In words, the first law says that the negation ($\neg$) of a disjunction ($A \vee B$) is logically equivalent to the conjunction of the negations of the individual statements A and B. The second law is similar, except we exchange conjunction for disjunction and vice-versa.

Exercise Verify the De Morgan law for disjunction by showing the logical equivalence of the left and right hand sides using a truth table:
Solution

$\neg$	$(A$	$\vee$	$B)$	$\Longleftrightarrow$	$(\neg$	$A)$	$\wedge$	$(\neg$	$B)$
F	T	T	T	T	F	T	F	F	T
F	T	T	F	T	F	T	F	T	F
F	F	T	T	T	T	F	F	F	T
T	F	F	F	T	T	F	T	T	F

We note that for any value of statements A and B, the values under the column for $\Longleftrightarrow$ are all true, indicating that both expressions $\neg (A \vee B)$, $(\neg A) \wedge (\neg B)$ have the same truth tables, as required.

Another useful logical equivalence is the following "contrapositive" form of implication, which we explore in the next exercise:

Exercise Show that $(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)$ is a tautology, i.e. this means that $A \Longrightarrow B$ is logically equivalent (LE) to $\neg B \Longrightarrow \neg A$.

Solution

$(A$	$\Longrightarrow$	$B)$	$\Longleftrightarrow$	$(\neg$	B	$\Longrightarrow$	$\neg$	$A)$
T	T	T	T	F	T	T	F	T
T	F	F	T	T	F	F	F	T
F	T	T	T	F	T	T	T	F
F	T	F	T	T	F	T	T	F

To show a situation where expressions are not logicaly equivalent, the following exercise may be considered:

Exercise Show $A \Longrightarrow B$ is not logically equivalent to $B \Longrightarrow A$

Solution

$(A$	$\Longrightarrow$	$B)$	$\Longleftrightarrow$	$(B$	$\Longrightarrow$	$A)$
T	T	T	T	T	T	T
T	F	F	F	F	T	T
F	T	T	F	T	F	F
F	T	F	T	F	T	F

Notice the middle column $\Longleftrightarrow$ has false entries, so we don't have logical equivalency.

Another item of terminology is *Logical Implication*. Logical implication is when the expression $A \Longrightarrow B$ is a tautology. If the statements A and B are such that we only get true statements from $A \Longrightarrow B$, then A logically implies **(LI)** B. This was the situation with the earlier illustration where we had defined statements A and B such that $A = (a > 5), B = (a > 3)$ where a is some integer.

If A is logically equivalent (LE) to B, then A LI B and B LI A.

Exercise: Show $A \wedge (A \Longrightarrow B)$ logically implies B. This is called "Modus Ponens."

Solution

$(A$	$\wedge$	$(A$	$\Longrightarrow$	$B))$	$\Longrightarrow$	B
T	T	T	T	T	T	T
T	F	T	F	F	T	F
F	F	F	T	T	T	T
F	F	F	T	F	T	F

1.3 Zermelo-Fraenkel Axiomatic Set Theory

Set theory is at the foundation of mathematics. The reader should have some awareness of the axioms of set theory, although in practice it seems that one rarely sees a mathematical proof that explicitly cites these axioms. These axioms are referred to as the Zermelo-Frankel Axioms.

1.3.1 The Zermelo-Fraenkel Axioms

The following so-called Zermelo-Fraenkel Axioms of set theory are presented to help provide the reader a more comprehensive picture of mathematics foundations. This section is inspired by the set of YouTube lectures by Richard Borcherds (ZF Axioms)
(`https://www.youtube.com/playlist?list=PL8yHsr3EFj52EKVgPi-p50fRP2_SbG2oi`)
and also the book *Axiomatic Set Theory* by Paul Bernays. The definitions are adapted from Bernays.

We note that in the axioms below, the notion of *set* is undefined, as is the inclusion relation, $\in$. Furthermore, all elements or members of sets are sets themselves.

Axiom of Extensionality
If $s \subseteq t$ and $t \subseteq s$, then $s = t$ where s, t are sets and $\subseteq$ means *subset*.

We define subset by the following: If s and t are sets such that, for all x, $x \in s$ implies $x \in t$, s is called a subset of t, where x is a set element or member. Occasionally, we might use the notation $s \subset t$ to indicate a *proper subset* whereby there is an element in t that is not in s.

To recap: The axiom states what it means for two sets to be equal - namely they contain the same elements.

Axiom of Foundation
Every non-empty set s contains an element t such that s and t have no common element.

This axiom prevents an element of a set having an element which appears in the original set. For example, the set $s = \{s\}$ is not allowed.

Axiom of Pairing
For any two different sets a and b, the pair $\{a, b\}$, or $\{b, a\}$, exists.

Axiom of Union
For any set s which contains at least two elements, there exists the set whose elements are the elements of the elements of s.

This set is called the union of the elements of s and is denoted by $\cup s$.

Axiom of Infinity
There exists at least one set W with the properties:

- a) $\emptyset \in W$, where $\emptyset$ refers to the "empty set." - the set with no elements.
- b) if $x \in W$, then $\{x\} \in W$.

The interpretation of the above is that a set exists with a non-ending sequence of elements. For example, if we think of the infinite sequence of non-negative integers being encoded as follows: $0 = \emptyset, 1 = \{0\}, 2 = \{1\}, \ldots$, then we can have the corresponding infinite set $S = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots\}$ which is justified by the axiom.

Axiom of Power-set
For any set s, there exists the set whose elements are all subsets of s.

To take an example, consider the set $s = \{1, 2, 3\}$. Then the power-set is $P = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}, \emptyset\}$. The number of elements, also called the *cardinality*, in this case is given by 2^N, where N is the number of elements in the original set s. Thus, we have $2^{N=3} = 8$. We note that the empty set, $\emptyset$, is considered a subset of every set.

Axiom of Subsets (Note: Borcherds refers to this as "separation")
For any set s and any predicate P which is meaningful for all elements of s, there exists the set y that contains just those elements x of s which satisfy the predicate P.

For example, let $s = \{1, 2, 3, 4, 5\}$ and the predicate $P(x)$ be true whenever x is even. Then, we have the set $y = \{x \in s | P(x) true\} = \{2, 4\}$.

Axiom of Replacement
For every set s and every single-valued function f of one argument which is defined for all the elements of s, there exists the set that contains all $f(x)$ with $x \in s$.

Axiom of Choice
For every disjointed set t for which $\emptyset \notin t$, the Cartesian product $\mathfrak{P}t$ differs from the $\emptyset$.

We define a *disjointed set* by the following: If a set s contains at least two elements, and any two elements of s are mutually exclusive (i.e. these elements have no common elements themselves).

Theorem The *Cartesian product* of the elements of a disjointed set t, denoted $\mathfrak{P}t$ is the set whose elements are the sets which contain a single element

from each element of t. If $a, b, \ldots$ are the elements of t, the Cartesian product is also denoted by $a \times b \times \ldots$. *Note*: For those interested, this theorem is proved in Bernays.

To illustrate the applications of the above axioms to a proof, consider the following exercise.

Exercise Complete the proof of the following theorem (adapted from Bernays):

Theorem For every non-empty set t, there exists the set whose elements are common to all elements of t.
This set is called the *intersection* of the elements of t and is denoted by $\cap t$.

Proof: By the Axiom of Union, $s = \cup t$ exists and contains the elements of the elements of t. The predicate "x is contained in each element of t" defines, by the Axiom of **fill in the blank**, a subset of s which is the intersection $\cap t$.

Solution
Axiom of **Subsets**

The following exercise explores the Cartesian product.

Exercise According to Bernays, for a disjointed set t, one has the Cartesian product, $\mathfrak{P}t = \emptyset$ if $\emptyset \in t$. Prove this using the Cartesian Product Theorem stated above in Axiom of Choice section.

Solution According to the theorem, the Cartesian product is the set whose elements are the sets which contain a single element from each element of t. Since $\emptyset \in t$ and contains no elements, the Cartesian product must be empty since there is no set possible that contains the required one element from $\emptyset$.

1.3.2 Set Operations

In this section, we present some set operations that are useful in much of the remainder of this book. The reader may be familiar with some of the material, although perhaps not necessarily in the formalism presented. Concepts and proofs in mathematics are very frequently expressed in terms of set language to be precise, so utility with set operations is important. For example, in later sections, we will discuss algebraic structures such as "groups" which will be defined in terms of sets with certain properties.

The emphasis here will be to continue the development following the axiomatic approach, largely adapted from *Axiomatic Set Theory* by Patrick Suppes. Hopefully, this will illustrate some of the notation and concepts we have been developing in the previous sections.

Binary Relations

Definition: *R is a binary relation* $\iff (\forall x)(x \in R \implies (\exists y)(\exists z)(x = \langle y, z\rangle))$.

We note that in the above, $\langle y, z\rangle$ is called an *ordered pair* and is formally defined in set notation as $\langle y, z\rangle = \{\{y\}, \{y, z\}\}$. Note how the ordering is encoded. So we have that a relation is a set of ordered pairs.

The definition is read as "R is a binary relation if and only if for all x if x is in R, then there exists a y and there exists a z such that x is equal to the ordered pair $\langle y, z\rangle$."

It should be remembered that the phrases "if and only if" and the "if ... then" are used to refer to the truth tables for the corresponding symbols and not the casual english meaning. If desired, we could express the definition by using a truth table as we did previously to be completely clear.

Sometimes the following notation is used discussing relations: xRy. This is formally defined as $xRy \iff \langle x, y\rangle \in R$.

Consider the following example set which is a relation:

$$R = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 1, 3\rangle, \langle 3, 1\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle\}.$$

We have utilized the angle bracket notation for ordered pairs for simplicity. Observe that this relation, R, has some special properties. To begin with, this relation is called *symmetric* because if xRy is true then we have yRx true. For example, $\langle 1, 2\rangle \in R$ and $\langle 2, 1\rangle \in R$.

Exercise For the relation R defined above, verify that it is symmetric by explicitly listing the ordered pairs in question and their corresponding symmetric partners.

Solution
$\langle 1, 2\rangle, \langle 2, 1\rangle$
$\langle 2, 1\rangle, \langle 1, 2\rangle$
$\langle 1, 3\rangle, \langle 3, 1\rangle$
$\langle 3, 1\rangle, \langle 1, 3\rangle$
$\langle 2, 3\rangle, \langle 3, 2\rangle$
$\langle 3, 2\rangle, \langle 2, 3\rangle$

We consider as an exercise, the proof that $\emptyset$ is a relation.

Exercise Prove that $\emptyset$ (the empty set) is a relation by appealing to the definition of relation given earlier.
Solution
Recalling the definition: *R is a binary relation* $\iff (\forall x)(x \in R \implies (\exists y)(\exists z)(x =$

$\langle y, z\rangle)))$, we substitute $\emptyset$ for R and obtain:

$$\emptyset \textit{ is a binary relation} \iff (\forall x)(x \in \emptyset \implies (\exists y)(\exists z)(x = \langle y, z\rangle)).$$

Now, since $x \in \emptyset$ is false (the empty set contains no members), the statement $(x \in \emptyset \implies (\exists y)(\exists z)(x = \langle y, z\rangle))$ is true. Recall the truth table for $\implies$ whereby if the first term is false, the entire statement is true no matter what the second term is. Therefore, we have shown the $\emptyset$ is a relation because it satisfies the definition.

Ordering Relations

In the previous section, we introduced the idea of a *symmetric* relation. We now present a more complete list of such definitions:

- R *is reflexive in* $A \iff (\forall x)(x \in A \implies xRx)$.
- R *is irreflexive in* $A \iff (\forall x)(x \in A \implies \neg(xRx))$.
- R *is symmetric in* $A \iff (\forall x)(\forall y)(x, y \in A \wedge xRy \implies yRx)$.
- R *is asymmetric in* $A \iff (\forall x)(\forall y)(x, y \in A \wedge xRy \implies \neg(yRx))$.
- R *is antisymmetric in* $A \iff (\forall x)(\forall y)(x, y \in A \wedge xRy \wedge yRx \implies x = y)$.
- R *is transitive in* $A \iff (\forall x)(\forall y)(\forall z)(x, y, z \in A \wedge xRy \wedge yRz \implies xRz)$.
- R *is connected in* $A \iff (\forall x)(\forall y)(x, y \in A \wedge x \neq y \implies xRy \vee yRx)$.
- R *is strongly connected in* $A \iff (\forall x)(\forall y)(x, y \in A \implies xRy \vee yRx)$.

A couple of items regarding notation. The notation $x, y \in A$ means $x \in A \wedge y \in A$. Also, by convention, the $\wedge$ and $\vee$ operations are performed before $\implies$ which saves writing extra parentheses in the definitions. For example, if we explicitly included the parentheses in the definition of symmetric to indicate order of operations, it would appear as $A(\forall x)(\forall y)(\big(x, y \in A \wedge xRy\big) \implies yRx)$.

If we consider the definition of *symmetric* above, we see how this corresponds to the example symmetric relation in the previous section. The reader should be cautioned to carefully observe the difference between *asymmetric* and *antisymmetric* relations.

Exercise Prove that the relation from the previous section is irreflexive by appealing to the definition. Define the set $A = \{1, 2, 3\}$ for purposes of this exercise.

Solution

Recalling R:

$$R = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 1,3\rangle, \langle 3,1\rangle, \langle 2,3\rangle, \langle 3,2\rangle\}.$$

we see that $\forall x \in A$, namely $1, 2, 3$, we are missing the corresponding ordered pairs $\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle$ in the relation R. Now if we consider the definition of *irreflexive* we have: R *is irreflexive in* $A \iff (\forall x)(x \in A \implies \neg(xRx))$. Clearly, xRx is false for any choice of $x \in A$, thus we have have $\neg(xRx)$ true for all choices of $x \in A$ and we see that R is therefore indeed *irreflexive*.

Exercise Show by counterexample, that the relation from the previous section is not *transitive*. Once again, consider the set $A = \{1, 2, 3\}$ for purposes of this exercise.

Solution

Recalling the definition: R *is transitive in* $A \iff (\forall x)(\forall y)(\forall z)(x, y, z \in A \wedge xRy \wedge yRz \implies xRz)$, we see that if we can find an instance where $x, y, z \in A \wedge xRy \wedge yRz \implies xRz$ is false, we are done. Consider $1R2$ and $2R1$ which are both true. However, $1R1$ is false because $\langle 1,1\rangle \notin R$. Therefore, we conclude that R is not transitive.

The following two definitions are important:

- R *is a partial ordering of* $A \iff R$ *is reflexive, anti-symmetric and transitive in* A.
- R *well-orders* $A \iff R$ *is connected in* $A \wedge (\forall B)(B \subseteq A \wedge B \neq \emptyset \implies B$ *has an* R*-minimal element*).

The definition of *R-minimal element* mentioned above is as follows: x *is an* R*-minimal element of* $A \iff x \in A \wedge (\forall y)(y \in A \implies \neg(yRx))$.

Let us examine the above two ordering definitions with some examples. Firstly, let us consider *partial ordering*. We will take $A = \{1, 2, 3\}$ and construct an appropriate relation. We can begin with taking all possible ordered pairs which gives us the following provisional relation:

$$R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \langle 3,3\rangle\}$$

The above relation is symmetric, because it contains $\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle$. The anti-symmetric requirement restricts the ordered pair partners. For example, if we have $\langle 1,2\rangle$ we cannot have $\langle 2,1\rangle$. So, let us remove those ordered pairs where the second element is smaller than the first:

$$R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,3\rangle\}$$

Lastly, we need to verify transitivity:
$1R1 \wedge 1R1 \implies 1R1$
$1R1 \wedge 1R2 \implies 1R2$

$1R1 \wedge 1R3 \Longrightarrow 1R3$
$1R2 \wedge 2R2 \Longrightarrow 1R2$
$1R2 \wedge 2R3 \Longrightarrow 1R3$
$1R3 \wedge 3R3 \Longrightarrow 1R3$
$2R2 \wedge 2R2 \Longrightarrow 2R2$
$2R2 \wedge 2R3 \Longrightarrow 2R3$
$2R3 \wedge 3R3 \Longrightarrow 2R3$
$3R3 \wedge 3R3 \Longrightarrow 3R3$

So, our revised R is a partial ordering of the set A. When dealing with real numbers, the symbol $\leq$ (less than or equal to) represents a partial ordering relation. The relation R we constructed above parallels this.

Now, let us do a similar construction to obtain a well-ordering. Again, consider the set $A = \{1, 2, 3\}$ and let us construct a relation R that satisfies the definition. To begin with, we can take as provisional all possible ordered pairs:

$$R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \langle 3,3\rangle\}$$

Now, we first need to make sure that R is *connected* in A by appealing to the definition of connected: R *is connected in* $A \Longleftrightarrow (\forall x)(\forall y)(x, y \in A \wedge x \neq y \Longrightarrow xRy \vee yRx)$. We have as members of R, $\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,3\rangle$, so R is connected.

Next, we need to verify the second part of the definition: $(\forall B)(B \subseteq A \wedge B \neq \emptyset \Longrightarrow B$ *has an* R*-minimal element*). There are seven subsets of A (we don't need to consider $\emptyset$), which are listed here:
$\{1\}$
$\{2\}$
$\{3\}$
$\{1, 2\}$
$\{1, 3\}$
$\{2, 3\}$
$\{1, 2, 3\}$

For 1 to be an R*-minimal* in B, we must remove $\langle 1,1\rangle$ from R. Similar, arguments apply to $\langle 2,2\rangle$ and $\langle 3,3\rangle$ corresponding to $\{2\}$ and $\{3\}$. Now, for $\{1, 2\}$ we must remove $\langle 2,1\rangle$ from R so that 1 is R*-minimal* in $\{1, 2\}$, and likewise for $\{1, 3\}$ we remove $\langle 3,1\rangle$. Similarly, we remove $\langle 3,2\rangle$ corresponding to $\{2, 3\}$. Now, $\{1, 2, 3\}$ has an R*-minimal* element already, so we are done. Our revised relation R is now:

$$R = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,3\rangle\}$$

This revised relation R well-orders A. This parallels the $<$ (less than) relation in real numbers.

Exercise There is a theorem in Suppes (Theorem 62) as follows: *R well-orders $A \implies$ R is asymmetric and transitive in A.* Verify the relation R above satisfies this theorem.

Solution. We first verify that R is asymmetric. We have $\langle 1,2\rangle$ but not $\langle 2,1\rangle$, $\langle 1,3\rangle$ but not $\langle 3,1\rangle$, and lastly $\langle 2,3\rangle$ but not $\langle 3,2\rangle$. Now, we verify transitivity: The only statement that makes sense is $1R2 \wedge 2R3 \implies 1R3$ which is true. Therefore, we have verified that R satisfies the theorem.

Equivalence Relations

We now discuss some important concepts that will appear in some form later, notably in abstract algebra. The reader will benefit by getting comfortable with these topics as early as possible, so we present them here.

- Definition: *R is an equivalence relation* $\iff$ *R is a relation* $\wedge$*R is reflexive, symmetric, and transitive.*
- Definition: the *R-coset of x* is defined by $R[x] = \{y | xRy\}$.
- Definition: Π *is a partition of* $A \iff \cup\Pi = A \wedge (\forall B)(\forall C)(B \in \Pi \wedge C \in \Pi \wedge B \neq C \implies B \cap C = \emptyset) \wedge (\forall x)(x \in \Pi \implies (\exists y)(y \in x))$.

A *partition* of a set is an exhaustive, mutually exclusive decomposition of a set into subsets, whose union is the set itself. For example, if our set is $A = \{1,2,3\}$, then a partition might be $\Pi = \{\{1\},\{2\},\{3\}\}$ or perhaps $\Pi = \{\{1\},\{2,3\}\}$.

We can see the partitioning through an example. Let us consider a set $A = \{1,2,3,4,5\}$ and construct an equivalence relation, R. Firstly, we know that R must be reflexive, so we provisionally begin with:

$$R = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle \langle 4,4\rangle \langle 5,5\rangle\}$$

We could actually stop here, because R happens to also be symmetric and transitive. However, to make the example slightly more complex, let us add some more members that are symmetric:

$$R = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle \langle 4,4\rangle \langle 5,5\rangle\}$$

where is can be seen that $\langle 1,2\rangle$ and $\langle 2,1\rangle$ have been added.
Now we need to verify that transitivity is satisified:
$1R1 \wedge 1R1 \implies 1R1$
$1R1 \wedge 1R2 \implies 1R2$
$1R2 \wedge 2R1 \implies 1R1$
$1R2 \wedge 2R2 \implies 1R2$
$2R1 \wedge 1R1 \implies 2R1$
$2R1 \wedge 1R2 \implies 2R2$
$2R2 \wedge 2R1 \implies 2R1$

$2R2 \wedge 2R2 \Longrightarrow 2R2$
$3R3 \wedge 3R3 \Longrightarrow 3R3$
$4R4 \wedge 4R4 \Longrightarrow 4R4$
$5R5 \wedge 5R5 \Longrightarrow 5R5$

Now, let us determine the *R-coset of* x for each $x \in A$:
$R[1] = \{1, 2\}$
$R[2] = \{1, 2\}$
$R[3] = \{3\}$
$R[4] = \{4\}$
$R[5] = \{5\}$

Now, we can form a set of all the cosets, which will be a partition of A:
$\Pi = \{\{1, 2\}, \{3\}, \{4\}, \{5\}\}$.

Functions

To help motivate the discussion of *functions*, which presumably many readers will have encountered previously and have a fair degree of experience with, within the set theoretical framework, the following directly quoted passage from Suppes (p.86) may be helpful:

"Since the eighteenth century, clarification and generalization of the concept of a function have attracted much attention. Fourier's representation of 'arbitrary' functions (actually piecewise continuous ones) by trigonometric series encountered much opposition; and later when Weierstrass and Riemann gave examples of continuous functions without derivatives, mathematicians refused to consider them seriously. Even today many textbooks of the differential and integral calculus do not give a mathematically satisfactory definition of functions. An exact and completely general definition is immediate within our set-theoretical framework. A function is simply a many-one relation, that is, a relation which to any element in its domain relates exactly one element in its range."

We now present the formal definition:

Definition: f *is a function* $\Longleftrightarrow$ f *is a relation* $\wedge(\forall x)(\forall y)(\forall z)(xfy \wedge xfz \Longrightarrow y = z)$.

Here is an example from Suppes which we use as an exercise.

Exercise Argue that the following relation is not a function: $f = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 3, 4\rangle\}$.

Solution:
Appealing to the definition of function, we see that the statement $1f1 \wedge 1f2 \Longrightarrow 1 = 2$ is false, therefore we conclude f is not a function. In other words, the

ordered pairs $\langle 1,1\rangle$ and $\langle 1,2\rangle$ which appear in f have the same first element, 1, but different second elements, 1 and 2, which is not allowed for a function.

Composition of functions is an important concept that appears quite frequently in some of the later topics. The notation for this is $(f \circ g)(x) = f(g(x))$, where f and g are functions, x is an element of a set, and the circle indicates composition. In words, we can think of this as a chain, whereby, firstly the mapping is applied using the the g function, then the result of this is mapped via the f function. Suppes states a formal definition of composition using something called the *relative product*, so for completeness we provide the definitions correspondingly:

Definition: $f \circ g = g/f$.

The relative product is given by the notation g/f and is defined by the following:

Definition: $g/f = \{\langle x,y\rangle \| (\exists z)(xgz \wedge zfy)\}$.

Exercise Given the two functions $f = \{\langle 3,2\rangle, \langle 4,5\rangle, \langle 6,7\rangle\}$ and $g = \{\langle 1,3\rangle, \langle 2,6\rangle\}$, determine the composition $f \circ g$ using the definition g/f.

Solution:
Let us pair up the terms xgz and zfy (in that order), where z is common to both:
$\langle 1,3\rangle, \langle 3,2\rangle$
$\langle 2,6\rangle, \langle 6,7\rangle$

Then we have $g/f = \{\langle 1,2\rangle, \langle 2,7\rangle\}$.

Exercise Prove the following theorem (which is actually part of "Theorem 82" in Suppes): *f and g are functions $\Longrightarrow$ $f \circ g$ is a function* .

Solution:
From the definition of a function provided earlier, we need to establish that $h = f \circ g$ is a relation, and also prove that $(\forall x)(\forall y)(\forall z)(xhy \wedge xhz \Longrightarrow y = z)$. For the first part, we appeal to the definition $f \circ g = g/f$ and subsequently note that the definition of g/f is a set of ordered pairs, which is a (binary) relation, also by definition.
For the second part, we need to show: $(\forall x)(\forall y)(\forall z)(xhy \wedge xhz \Longrightarrow y = z)$. Now consider xhy. From the definition of relative product, this means that $(\exists w)(xgw \wedge wfy)$, and likewise for xhz this means that $(\exists w')(xgw' \wedge w'fz)$. Rewriting the hypothesis, we obtain: $(\forall x)(\forall y)(\forall z)((\exists w)(xgw \wedge wfy) \wedge (\exists w')(xgw' \wedge w'fz))$. Now, since g is a function, this implies that $w = w'$. Then, since f is a function and $w = w'$, this implies $y = z$ thereby completing the proof.

We now define the concept of a converse relation, denoted $\breve{R}$, which will be

immediately useful in what comes next.

Definition: $\breve{R}= \{\langle x, y\rangle | yRx\}$, where R is a relation.

The following definitions are key:

- Definition: *f is 1-1* $\iff$ *f and $\breve{f}$ are functions* .
- Definition: *f is 1-1* $\implies f^{-1} = \breve{f}$, where f^{-1} is the *inverse* of f.

We note that "1-1" is read "one-to-one." We now illustrate a counter-example to a 1-1 function.

Exercise Show that the following function, $f = \{\langle 1, 2\rangle, \langle 2, 2\rangle, \langle 3, 4\rangle\}$ is not 1-1.
Solution: Let us first determine the converse relation to f: $\breve{f}= \{\langle 2, 1\rangle, \langle 2, 2\rangle, \langle 4, 3\rangle\}$. We see that this relation is not a function because the elements $\langle 2, 1\rangle, \langle 2, 2\rangle$ have the same first entry, but different second entries. Therefore, we conclude f is not 1-1.

We now introduce some additional terminology:

- Definition: Domain of a relation R: $\mathcal{D}R = \{x|(\exists y)(xRy)\}$
- Definition: Range of a relation R: $\mathcal{R}R = \{y|(\exists x)(xRy)\}$. This is also referred to as the *counterdomain* or *converse domain*.
- Definition: *f is a function from set A <u>into</u> set B* $\iff$ *f is a function* $\wedge$ $\mathcal{D}f = A \wedge \mathcal{R}f \subseteq B$.
- Definition: *f is a function from set A <u>onto</u> set B* $\iff$ *f is a function* $\wedge$ $\mathcal{D}f = A \wedge \mathcal{R}f = B$.
- Definition: *Restriction* of the domain of a relation R to a given set A: $R|A = R \cap (A \times \mathcal{R}R)$.
- Definition: the *image* of the set A under R: $R\text{“}A = \mathcal{R}(R|A)$.

Exercise What is the image of $A = \{1, 2, 4, 6\}$ under $R = \{\langle 1, 10\rangle, \langle 2, 11\rangle, \langle 5, 15\rangle\}$?

Solution: First, let us determine the restriction $R|A$. We need to obtain the Cartesian product $A \times \mathcal{R}R$ which is:

$$\{\langle 1, 10\rangle, \langle 1, 11\rangle, \langle 1, 15\rangle, \langle 2, 10\rangle, \langle 2, 11\rangle, \langle 2, 15\rangle, \langle 4, 10\rangle, \langle 4, 11\rangle, \langle 4, 15\rangle, \langle 6, 10\rangle, \langle 6, 11\rangle, \langle 6, 15\rangle\}$$

Next, we determine the intersection with R:

$$R|A = R \cap (A \times \mathcal{R}R) = \{\langle 1, 10\rangle, \langle 2, 11\rangle\}$$

Lastly, we obtain the image of A under R:

$$R\text{“}A = \mathcal{R}(R|A) = \{10, 11\}$$

It should be kept in mind that we are always dealing with sets when we refer to functions now and later in the material, so if there is any confusion, the reader should always consult the pertinent definitions to see exactly what sets or subsets are being referenced in any manipulations or results. For example, does a particular operation involve the entire set or only some portion of a set. Typically, engineers and scientists may normally think of functions in terms of graphs on a say two-dimensional plot, but in the pure mathematical context, keeping in mind the underlying set framework as has been outlined in the above material is important.

1.4 Peano Axioms of Arithmetic

In the previous section, we built up a basic framework for set theory based on the Zermelo-Frankel axioms. We now establish the foundations of the natural numbers, founded on top of that set theory, by stating the Peano Axioms. Much of this material is based directly on *Schaum's Outline of Theory and Problems of Abstract Algebra* by Frank Ayres and Lloyd R. Jaisingh.

Let there exist a non-empty set $\mathbb{N}$ such that:

- Axiom I: $1 \in \mathbb{N}$.
- Axiom II: For each $n \in \mathbb{N}$ there exists a unique $n^* \in \mathbb{N}$, called the *successor* of n.
- Axiom III: For each $n \in \mathbb{N}$ we have $n^* \neq 1$.
- Axiom IV: If $m, n \in \mathbb{N}$ and $m^* = n^*$, then $m = n$.
- Axiom V: Any subset K of $\mathbb{N}$ having the properties (a) $1 \in K$, (b) $k^* \in K$ whenever $k \in K$ is equal to $\mathbb{N}$.

We now define addition and multiplication on $\mathbb{N}$.

Addition:
(i) $n + 1 = n^*$, for every $n \in \mathbb{N}$
(ii) $n + m^* = (n + m)^*$, whenever $n + m$ is defined.

We then have the following laws for addition. For all $m, n, p \in \mathbb{N}$:

- Closure: $n + m \in \mathbb{N}$
- Commutative: $n + m = m + n$

- Associative: $m + (n + p) = (m + n) + p$
- Cancellation: If $m + p = n + p$, then $m = n$

Exercise Suppose we have two natural numbers, n, m, whereby $n = 1, m = 1^*$. For this restricted case, prove the commutative law for addition: $n + m = m + n$.
Solution:
We have that $n+m = 1+1^*$. Now, from the definition of addition (ii), we obtain $1+1^* = (1+1)^*$. From the definition of addition (i), we obtain $(1+1)^* = (1^*)^*$. Finally, $(1^*)^* = 1^*+1$ from the definition of addition (i) which is equal to $m+n$, thus completing the proof.

Multiplication:
(i) $n \cdot 1 = n$
(ii) $n \cdot m^* = n \cdot m + n$, whenever $n \cdot m$ is defined.

Similar to addition, we have laws for multiplication. For all $m, n, p \in \mathbb{N}$:

- Closure: $n \cdot m \in \mathbb{N}$
- Commutative: $m \cdot n = n \cdot m$
- Associative: $m \cdot (n \cdot p) = (m \cdot n) \cdot p$
- Cancellation: If $m \cdot p = n \cdot p$, then $m = n$.

If we consider both addition and multiplication, there are so-called distributive laws. For all $m, n, p \in \mathbb{N}$:

- D_1: $m \cdot (n + p) = m \cdot n + m \cdot p$
- D_2: $(n + p) \cdot m = n \cdot m + p \cdot m$.

The reader should be cautioned or reminded at this point that the order of the variables and operations in laws such as in the above are important to observe in general. With certain mathematical objects that we will consider, such as *groups*, swapping the positions of variables may not necessarily yield the same results. Therefore, one must carefully consider the definitions relevant to each mathematical object in question.

Exercise How are we justified in asserting that $m \cdot n = n \cdot m$, when $m, n \in \mathbb{N}$?
Solution: The commutative law for multiplication under $\mathbb{N}$ provides the justification.

Exercise Suppose we have $m, n \in \mathbb{N}$ and form the product $p = n \cdot m$. Is the result $p \in \mathbb{N}$?

Solution: Yes. The closure law for multiplication under $\mathbb{N}$ provides the justification.

Note in the above exercises, even though we may have some intuitive sense for the reasons, we must appeal to an exact statement which justifies the assertion. This may be an axiom, definition, theorem, law etc. which has been established for the objects in question. This habit will be useful to form as we consider other contexts in pure mathematics.

1.5 Gödel Theorems

To provide a more complete picture to the reader regarding the underpinnings of mathematics and logic, it is useful to consider the important results by Gödel which are cited in this context. The section is largely adapted from entries in *Stanford Encyclopedia of Philosophy*(https://plato.stanford.edu/entries/goedel/) and *Logic for Mathematicians* by A.G. Hamilton.

There are three theorems that we will consider. The first is called "the Completeness Theorem", the second is "the First Incompleteness Theorem", and the third is "The Second Incompleteness Theorem."

We begin with some definitions adapted from (https://plato.stanford.edu/entries/goedel-incompleteness/):

- *Formal system*: (Roughly) A system of axioms equipped with rules of inference, which allow one to generate new theorems.
- *Complete*: A formal system for which every statement of the system, either the statement or its negation can be derived ("proved") is complete.
- *Consistent*: A formal system for which there is no statement such that the statement and its negation are both derivable is consistent.

The Completeness Theorem

Every valid logical expression is provable. Equivalently, every logical expression is either satisfiable or refutable.

An illustration of how this works is provided in the Stanford reference mentioned earlier, which is reproduced here.
Suppose we have a logical expression $\phi = \forall x_0 \exists x_1 \psi(x_0, x_1)$. We can transform that expression with quantifiers into a list of expressions without quantifiers:

$$\begin{aligned}
\phi_0 &= \psi(x_0, x_1) \\
\phi_1 &= \psi(x_0, x_1) \wedge \psi(x_1, x_2) \\
&\dots \\
\phi_n &= \psi(x_0, x_1) \wedge \ldots \wedge \psi(x_n, x_{n+1})
\end{aligned}$$

Then, there are two cases:
Case 1: For some n, ϕ_n is not satisfiable. This implies the original ϕ is refutable (its negation is provable).
Case 2: Each ϕ_n is satisfiable. This implies the original ϕ is satisfiable.

The Stanford reference states that "logical expression" in the terminology of the theorem is "a well-formed first order formula without identity." Gödel's 1929 dissertation *On the Completeness of the Calculus of Logic* which is the source of the theorem, states the following:
"The main object of the following investigations is the proof of the completeness of the axiom system for what is called the restricted functional calculus, namely the system given in *Whitehead and Russell 1910*, Part I, *1 and *10, and, in a similar way, in *Hilbert and Ackermann 1928* (hereafter cited as H.A.) , III, §5." (Source: Kurt Gödel *Collected Works* Vol.1 by Feferman, et al. (1986) - Page 61.)

The notation and axioms for this system are then specified in the same reference. Briefly, the logic symbols are the same we have seen previously, namely: $\vee, \wedge, \Longrightarrow, \Longleftrightarrow, \neg$ and the axioms are as follows:

- (1) $X \vee X \Longrightarrow X$
- (2) $X \Longrightarrow X \vee Y$
- (3) $X \vee Y \Longrightarrow Y \vee X$
- (4) $(X \Longrightarrow Y) \Longrightarrow (Z \vee X \Longrightarrow Z \vee Y)$
- (5) $(\forall x) F(x) \Longrightarrow F(y)$
- (6) $(\forall x)[X \vee F(x)] \Longrightarrow X \vee (\forall x) F(x)$

The notation $F(x)$ above refers to a "predicate" that can be true or false depending on the value of x. For example, $F(x)$ can be true if $x \in A$, where A is some set.

There are also rules of inference, one of which is the "modus ponens" introduced previously. Namely, $(p \wedge (p \Longrightarrow q)) \Longrightarrow q$ where p and q are statements that can be true or false.

Exercise In the text of Gödel's dissertation, it is stated that $\Longrightarrow$ is used as an abbreviation. Also, it is implied that only $\vee$ and $\neg$ are necessary in order to represent the needed logic. Substantiate this by showing that it is possible to obtain the truth table for $\Longrightarrow$ only using $\vee$ and $\neg$.
Solution:

Recalling the truth table for $\Longrightarrow$:

A	$\Longrightarrow$	B
T	T	T
T	F	F
F	T	T
F	T	F

we can see by inspection that if we negate the A column, and use $\vee$ instead of $\Longrightarrow$ we will reproduce the same truth table. To confirm, let us do this explicity:

$(\neg$	$A)$	$\vee$	B
F	T	T	T
F	T	F	F
T	F	T	T
T	F	T	F

Exercise Is the following logical expression provable (within the above axiom system): $(X \Longrightarrow Y) \vee (X \Longrightarrow Y) \Longrightarrow (X \Longrightarrow Y)$?

Solution: Yes, according to Gödel's Completeness Theorem, since the formula is valid (taking "valid" to mean true for any combination of true or false for the variables X and Y). In fact, in this case it was obtained from Axiom (1) by substituting $X \Longrightarrow Y$ for X, immediately verifying the completeness theorem.

It is worth emphasizing the following point, raised by Gödel in his dissertation. Namely, since the logical axioms are valid and the rules of inference preserve truth, this means that every provable formula (i.e. derived from the axioms using the rules of inference) is valid. Gödel's Completeness Theorem actually states the converse: *Every valid logical expression is provable.* Again, this is within the specific system described above.

The First Incompleteness Theorem

To introduce this section and the next, the following quote from the *Stanford Encyclopedia of Philosophy* entry on Gödel (https://plato.stanford.edu/entries/goedel/) may be illuminating:
"The First Incompleteness Theorem provides a counterexample to completeness by exhibiting an arithmetic statement which is neither provable nor refutable in Peano arithmetic, though true in the standard model. The Second Incompleteness Theorem shows that the consistency of arithmetic cannot be proved

in arithmetic itself."

It is hoped that the previous sections on Peano Axioms and the Completeness Theorem will provide a good starting point for considering these incompleteness theorems.

We now present the First Incompleteness Theorem, based on the entry in the *Stanford Encyclopedia of Philosophy* for Gödel Incompleteness (https://plato.stanford.edu/entries/goedel incompleteness/):

Any consistent formal system F within which a certain amount of elementary arithmetic can be carried out is incomplete; i.e., there are statements of the language of F which can neither be proved nor disproved in F.

At this point, it is useful to introduce the concept of *Gödel numbering* (ref: https://plato.stanford.edu/entries/goedel-incompleteness/sup1.html), which provides a procedure for encoding components of a formal system as natural numbers. The idea is that certain statements can be represented by a number and reasoned about as a number. For example, the statement (Axiom (1) from previous section) $X \vee X \implies X$ might be represented as a natural number like 1329487 and so forth.

To see how Gödel numbers are determined is a unambiguous fashion, we proceed in two steps. Firstly, each symbol of the "language" of the formal system is given a natural number code. For example: the symbol '0' might be assigned code number 1, the plus sign '+' might be 3, the equals sign, '=' might be 4, a variable x_1 might be 13, and $>$ is 14.
The next step is to encode a particular formula, which is a sequence of code numbers, into a final encoded natural number. This is done (apparently following Gödel's original method), by leveraging the prime numbers and the fundamental theorem of arithmetic, which states that every natural number greater than one has a unique prime factorization (up to order of the factors). This means that a given sequence of symbols will have a unique representation in this prime encoding scheme.
Let us represent the primes as $p_1, p_2, p_3, \ldots, p_n, \ldots$. The first few primes in order are: $2, 3, 5, 7, 11$. The next step is to raise each prime to the power of the corresponding symbol code at that position in the symbol sequence. For example, let us take the symbol sequence: $0 + 0 = 0$. The code sequence for this, using our above mapping, is: $1, 3, 1, 4, 1$. To do the final encoding with the primes, we compute $p_1^1 \times p_2^3 \times p_3^1 \times p_4^4 \times p_5^1 = 2^1 \times 3^3 \times 5^1 \times 7^4 \times 11^1 = 2 \times 27 \times 5 \times 2401 \times 11 = 7130970$. So this final result, 7130970, would be the Gödel number for the formula $0 + 0 = 0$.

Exercise Using the above symbol encoding, give an argument for why just representing a given formula by the symbol code sequence is not enough to guarantee a unique Gödel number.

Solution: Consider the formulas $0 + 0 = 0$ vs. $x_1 > 0$. Supposing that both of these are meaningful formulas, we can see that the code sequence for both would be the same, namely: 13141. Therefore, if we left the encoding this way, given the number 13141 we would not be able to determine which of those two formulas was being represented. However, if we do the second step of the process of encoding involving the primes, we would obtain for $x_1 > 0$ the following Gödel number: $2^{13} \times 3^{14} \times 5^1 = 8192 \times 4782969 \times 5 = 195910410240$, which is obviously distinct from 7130970.

Now we have established the concept of Gödel Numbering, we can continue the discussion. In particular, in addition to assigning Gödel numbers to individual formulas, we can imagine assigning a Gödel number to the proof of a formula. If we think of a proof as a sequence of formulas, starting from axioms, applying the inference rules and other logical operations defined in the formal system, we can convert this proof to a Gödel number. For example, taking the *modus ponens* inference rule, suppose we might have something like this $X, X \Longrightarrow Y, Y, (\neg Y) \Longrightarrow Z$, where we are trying to prove $(\neg Y) \Longrightarrow Z$. Suppose that X and $X \Longrightarrow Y$ are our axioms, then the above sequence could be considered a proof of $(\neg Y) \Longrightarrow Z$.
As we did before, we can convert each symbol of the eleven symbol sequence to its code number, say: $123, 123, 11, 125, 125, 15, 13, 125, 17, 11, 127$ and then encode to a Gödel number using the primes: $2^{123} \times 3^{123} \times \ldots p_{11}^{127}$, where p_{11} is the eleventh prime, 31.

With this in mind, we can then construct the formula which Gödel showed could not be proved or disproved in the particular formal system at hand. Following the Hamilton logic book reference, we define a formula $\mathcal{U}$ in words as follows: for every natural number n, n is not the Gödel number of a proof of the formula $\mathcal{U}$. To clarify, Gödel's theorem states that $\mathcal{U}$ is not a theorem in the formal system, and neither is $\neg(\mathcal{U})$.

Another concept that is useful in this context is *recursive functions*. For those with experience in computer science and software development, the idea of recursive functions may be familiar. According to the Hamilton reference, recursive functions can be constructed from three basic function and three rules which we provide below. Note that the convention used in Hamilton's reference that the set of natural numbers starts with 0 as opposed to 1, and the symbol D_N is used to represent this set of natural numbers starting from 0. The symbol D_N^k then represents a k-dimensional cartesian product set of natural numbers. For example, $D_N^2 = \{\langle 0, 0\rangle, \langle 1, 0\rangle, \langle 2, 0\rangle, \ldots\}$, and then $\langle 2, 3\rangle$ and $\langle 5, 11\rangle$ are two particular elements of that set.

The basic functions are:

- 1. The zero function $z : D_N \to D_N$, given by $z(n) = 0$ for every $n \in D_N$. The notation $z : D_N \to D_N$ is read as "z is the function which maps

elements in D_N to D_N". Note that the arrow is not the same and the logical implication $\Longrightarrow$ previously discussed. So in this case, the function z maps (i.e. connects) every natural number in D_N to the natural number 0.

- 2. The successor function $s : D_N \to D_N$, given by $s(n) = n + 1$ for every $n \in D_N$.
- 3. The projection functions $p_i^k : D_N^k \to D_N$, given by $p_i^k(n_1, \ldots, n_k) = n_i$, for every $n_1, \ldots, n_k \in D_N$.

The rules are as follows:

- R1. Composition. If $g : D_N^j \to D_N$ and $h_i : D_N^k \to D_N$ for $1 \leq i \leq j$, then $f : D_N^k \to D_N$, defined by $f(n_1, \ldots, n_k) = g(h_1(n_1, \ldots, n_k), \ldots, h_j(n_1, \ldots, n_k))$ is obtained by composition from g and $h_1, \ldots, h_j$.
- R2. Recursion. If $g : D_N^k \to D_N$ and $h : D_N^{k+2} \to D_N$, then the function $f : D_N^{k+1} \to D_N$, defined by $f(n_1, \ldots, n_k, 0) = g(n_1, \ldots, n_k)$, and $f(n_1, \ldots, n_k, n + 1) = h(n_1, \ldots, n_k, n, f(n_1, \ldots, n_k, n))$ is said to be obtained by recursion from g and h. We can also have recursion with all the n_i absent, as in $f(0) = a$ and $f(n + 1) = h(n, f(n))$, where a is a fixed member of D_N.
- R3. Least Number Operator. Let $g : D_N^{k+1} \to D_N$ be any function with the property that for each $n_1, \ldots, n_k \in D_N$ there is at least one $n \in D_N$ such that $g(n_1, \ldots, n_k, n) = 0$. Then the function $f : D_N^k \to D_N$, defined by $f(n_1, \ldots, n_k) =$ least number $n \in D_N$ such that $g(n_1, \ldots, n_k, n) = 0$, is said to be obtained from g by the use of the least number operator.

Let us consider some examples to illustrate the above functions and rules.

Taking the projection function p_2^3, we can apply it to $\langle 4, 6, 9\rangle$ and obtain $p_2^3(4, 6, 9) = 6$. This is the second value in the triplet $\langle 4, 6, 9\rangle$ extracted (or "projected").

Now, moving to composition, take $g(n_1, n_2, n_3) = n_1 n_2 + n_3$ and $h_1(m_1, m_2) = m_1 + m_2, h_2(m_1, m_2) = m_1 m_2, h_3(m_1, m_2) = m_1 + 2m_2$. Then, the composition is $f(m_1, m_2) = g(h_1(m_1, m_2), h_2(m_1, m_2), h_3(m_1, m_2)) = (m_1 + m_2)(m_1 m_2) + (m_1 + 2m_2)$.

Lastly, let us consider recursion. Let $h(m_1, m_2) = m_1 + m_2$ and $f(0) = 1$. Then, $f(1) = h(0, f(0)) = 0 + 1 = 1$, $f(2) = h(1, f(1)) = 1 + 1 = 2$, $f(3) = h(2, f(2)) = 2 + 2 = 4$, $f(4) = h(3, f(3)) = 3 + 4 = 7$, and so forth.

We now show that the "addition function", which is one of the basic operators in our formal system for arithmetic, is recursive. In other words, it can be constructed from the above basic functions and finite application of the rules.

We show how this example (taken from Hamilton) is done.

We want to show that the addition function $f_1(p,q) = p + q$ can be constructed as recursive. If we take the projection functions p_1^1, p_3^3, and the successor function s we can form the following:

$$\begin{aligned} f_1(m,0) &= p_1^1(m) \\ f_1(m,n+1) &= s(p_3^3(m,n,f_1(m,n)) \end{aligned}$$

Let's check this for $f_1(2,3)$ which we anticipate should be $2+3=5$. We start by working backwards from the final function:

$$\begin{aligned} f_1(2,3) &= s(p_3^3(2,2,f_1(2,2)) \\ f_1(2,2) &= s(p_3^3(2,1,f_1(2,1)) \\ f_1(2,1) &= s(p_3^3(2,0,f_1(2,0)) \\ f_1(2,0) &= p_1^1(2) = 2 \end{aligned}$$

We have reached the "base case" and now we can evaluate the function working in the forward direction:

$$\begin{aligned} f_1(2,0) &= p_1^1(2) = 2 \\ f_1(2,1) &= s(p_3^3(2,0,f_1(2,0)) = s(p_3^3(2,0,2)) = 3 \\ f_1(2,2) &= s(p_3^3(2,1,f_1(2,1)) = s(p_3^3(2,1,3)) = 4 \\ f_1(2,3) &= s(p_3^3(2,2,f_1(2,2)) = s(p_3^3(2,2,4)) = 5 \end{aligned}$$

Exercise Show how to construct the multiplication function, $f_2(m,n) = mn$ as a recursive, using the addition function, f_1 defined above recursively, as well as the appropriate projection functions.

Solution If we consider what mn means as an addition problem, this can give us a clue how to proceed. Namely, we know that $mn = \overbrace{m+m+\ldots+m}^{n}$. So, if we start with a base case of 0, and then add m to that base value n times, we should get the desired result. Putting this into the recursive format, and leveraging the addition function, f_1 defined earlier, we obtain:

$$\begin{aligned} f_2(m,0) &= z(m) = 0, \text{ where } z \text{ is the zero function defined earlier} \\ f_2(m,n+1) &= f_1(p_3^3(m,n,f_2(m,n)), p_1^3(m,n,f_2(m,n))) \end{aligned}$$

Let's check this for a simple case to see if it works. Take $f_2(3,5)$ which we expect should be 15. As before let us start by working backwards from the final function:

$$
\begin{aligned}
f_2(3,5) &= f_1(f_2(3,4),3) \\
f_2(3,4) &= f_1(f_2(3,3),3) \\
f_2(3,3) &= f_1(f_2(3,2),3) \\
f_2(3,2) &= f_1(f_2(3,1),3) \\
f_2(3,1) &= f_1(f_2(3,0),3) \\
f_2(3,0) &= 0
\end{aligned}
$$

We have reached the "base case", so now we can evaluate the function working in the forward direction:

$$
\begin{aligned}
f_2(3,0) &= 0 \\
f_2(3,1) &= f_1(f_2(3,0),3) = 0+3 = 3 \\
f_2(3,2) &= f_1(f_2(3,1),3) = 3+3 = 6 \\
f_2(3,3) &= f_1(f_2(3,2),3) = 6+3 = 9 \\
f_2(3,4) &= f_1(f_2(3,3),3) = 9+3 = 12 \\
f_2(3,5) &= f_1(f_2(3,4),3) = 12+3 = 15
\end{aligned}
$$

The Second Incompleteness Theorem

Chapter 2

Methods of Proof

2.1 Induction

2.1.1 Weak Induction

2.1.2 Strong Induction

2.2 Proof by Contradiction

Proof by contradiction is a very useful method of proof which is used quite frequently. The usual pattern is one assumes the converse of what is being asserted, and then following a sequence of logical deductions arriving at a contradiction. Once this contradiction has been uncovered, then it implies the original assumption must have been false thus completing the proof. Here is an example to illustrate the points.

Prove that there is no rational number whose square is 12. (Note: This was originally an exercise in Rudin PMA 3rd Edition).

Proof:

Suppose that there was a rational number whose square was 12**.** This means that

$$\left(\frac{p}{q}\right)^2 = 12$$

for integers p, q. We assume that p and q are not both even. In other words, all common factors of 2 have been cancelled. This can always been done for a rational number.

Upon expansion we obtain:

$$p^2 = 12q^2 = 2\left(6q^2\right)$$

This implies that p^2 and p are both even. Thus q is odd. So we write $p = 2m$ for integer m and obtain:

$$(2m)^2 = 4m^2 = 12q^2$$

This implies that

$$m^2 = 3q^2$$

Since q is assumed to be odd, q^2 is odd, and $3q^2$ is also odd. Now, m^2 must be therefore be odd, and likewise for m. Therefore, for integers r, n we can rewrite the above as:

$$(2r+1)^2 = 3(2n+1)^2$$

Now, expanding both sides yields:

$$4r^2 + 4r + 1 = 3\left(4n^2 + 4n + 1\right)$$

$$4r^2 + 4r + 1 = 12n^2 + 12n + 3$$

$$4r^2 + 4r = 12n^2 + 12n + 2$$

$$4r^2 + 4r = 12n^2 + 12n + 2$$

The left side is clearly divisible by 4.

$$r^2 + r = 3n^2 + 3n + \frac{2}{4}$$

The left side is an integer, but the right side is not, which is a contradiction. Therefore our assumption about both p, q not even is false. However, since this can always be done for the rational number p/q it implies that there is no rational p/q such that $(p/q)^2 = 12$.

2.3 Direct Proof

Index