

Pure Mathematics for Engineers and Scientists

Anthony Daniell

April 29, 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, Godel 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

1	Mathematical Foundations	7
1.1	Basic Notation	7
1.2	Mathematical Logic	8
1.3	Zermelo-Fraenkel Axiomatic Set Theory	11
1.3.1	The Zermelo-Fraenkel Axioms	12
1.3.2	Set Operations	14
1.4	Peano Axioms of Arithmetic	18
1.5	Godel Theorems	18
2	Methods of Proof	19
2.1	Induction	19
2.1.1	Weak Induction	19
2.1.2	Strong Induction	19
2.2	Proof by Contradiction	19
2.3	Direct Proof	20

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: $\dots, -2, -1, 0, 1, 2, 3, \dots$
- \mathbb{N} is the set of natural numbers: $0, 1, 2, 3, \dots$ (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, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ 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

$$\mathbb{Q} = \left\{ r \mid r = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0 \right\}$$

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 (\implies), If and Only If (\iff):

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	\implies	B
T	T	T
T	F	F
F	T	T
F	T	F

If and only if (Iff):

A	\iff	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 $A \implies B$ 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 (\implies).

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 $A \iff B$ is equivalent to $(A \implies B) \wedge (B \implies A)$.

Solution

$(A \mid \implies \mid B)$	\wedge	$(B \mid \implies \mid A)$
$T \mid T \mid T$	T	$T \mid T \mid T$
$T \mid F \mid F$	F	$F \mid T \mid T$
$F \mid T \mid T$	F	$T \mid F \mid F$
$F \mid F \mid F$	T	$F \mid T \mid F$

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 $A \iff B$ 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	$(A \mid \vee \mid B)$	\iff	$(\neg \mid A)$	\wedge	$(\neg \mid B)$
F	$T \mid T \mid T$	T	$F \mid T$	F	$F \mid T$
F	$T \mid T \mid F$	T	$F \mid T$	F	$T \mid F$
F	$F \mid T \mid T$	T	$T \mid F$	F	$F \mid T$
T	$F \mid F \mid F$	T	$T \mid F$	T	$T \mid F$

We note that for any value of statements A and B , the values under the column for \iff 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 $(A \implies B) \iff (\neg B \implies \neg A)$ is a tautology, i.e. this means that $A \implies B$ is logically equivalent (LE) to $\neg B \implies \neg A$.

Solution

$(A \implies B)$	\iff	$(\neg B \implies \neg A)$
T	T	T
T	F	F
F	T	T
F	T	F

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

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

Solution

$(A \implies B)$	\iff	$(B \implies A)$
T	T	T
T	F	F
F	T	T
F	T	F

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

Another item of terminology is *Logical Implication*. Logical implication is when the expression $A \implies B$ is a tautology. If the statements A and B are such that we only get true statements from $A \implies B$, 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 $A \wedge (A \implies B)$ logically implies B . This is called "Modus Ponens."

Solution

$(A \wedge (A \implies B))$	\implies	B
T	T	T
T	F	F
F	T	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-Fraenkel 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 Borchers (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: $0 = \emptyset, 1 = \{\emptyset\}, 2 = \{\emptyset, \{\emptyset\}\}, \dots$, then we can have the corresponding infinite set $S = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots\}$ 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 $P = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. 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: Borchers 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 $y = \{x \in s \mid P(x) \text{ true}\} = \{2, 4\}$.

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, \dots are the elements of t , the Cartesian product is also denoted by $a \times b \times \dots$. *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:

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

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 $A(\forall x)(\forall y)((x, y \in A \wedge xRy) \implies yRx)$.

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 $\neg(xRx)$ 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:

$$\begin{aligned} 1R1 \wedge 1R1 &\implies 1R1 \\ 1R1 \wedge 1R2 &\implies 1R2 \\ 1R1 \wedge 1R3 &\implies 1R3 \\ 1R2 \wedge 2R2 &\implies 1R2 \end{aligned}$$

$$1R2 \wedge 2R3 \implies 1R3$$

$$1R3 \wedge 3R3 \implies 1R3$$

$$2R2 \wedge 2R2 \implies 2R2$$

$$2R2 \wedge 2R3 \implies 2R3$$

$$2R3 \wedge 3R3 \implies 2R3$$

$$3R3 \wedge 3R3 \implies 3R3$$

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.

Equivalence Relations

Functions

1.4 Peano Axioms of Arithmetic

1.5 Godel Theorems

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:

$$p^2 = 12q^2 = 2(6q^2)$$

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:

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

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

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

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

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

antisymmetric, 16
asymmetric, 16

Cardinality, 13
connected, 16

De Morgan's Law's, 10
Dedekind Cuts, 7

irreflexive, 16

partial ordering, 17

R-minimal element, 17
reflexive, 16

Set builder notation, 8
strongly connected, 16
symmetric, 16

transitive, 16

well-order, 17