The Nuts and Bolts of Proofs
Contents

List of Symbols ........................................................................................................ vii

<table>
<thead>
<tr>
<th>CHAPTER 1</th>
<th>Getting Started ................................................................. 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction and Basic Terminology ........................................ 1</td>
</tr>
<tr>
<td></td>
<td>General Suggestions ................................................................ 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 2</th>
<th>Basic Techniques to Prove If/Then Statements ............................ 7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What Does “If/Then” Mean? ..................................................... 7</td>
</tr>
<tr>
<td></td>
<td>The Negation of a Statement: AND/OR ........................................ 16</td>
</tr>
<tr>
<td></td>
<td>Proof by Contrapositive ........................................................ 21</td>
</tr>
<tr>
<td></td>
<td>Proof by Contradiction ................................................................ 25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 3</th>
<th>Special Kinds of Theorems ..................................................... 33</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“If and Only If” or “Equivalence Theorems” .................................. 33</td>
</tr>
<tr>
<td></td>
<td>Use of Counterexamples ................................................................ 40</td>
</tr>
<tr>
<td></td>
<td>Mathematical Induction .............................................................. 42</td>
</tr>
<tr>
<td></td>
<td>Existence Theorems ...................................................................... 52</td>
</tr>
<tr>
<td></td>
<td>Uniqueness Theorems .................................................................... 54</td>
</tr>
<tr>
<td></td>
<td>Composite Statements.................................................................... 58</td>
</tr>
<tr>
<td></td>
<td>Multiple Hypotheses .................................................................... 58</td>
</tr>
<tr>
<td></td>
<td>Multiple Conclusions ................................................................... 61</td>
</tr>
<tr>
<td></td>
<td>Equality of Numbers .................................................................... 66</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 4</th>
<th>Some Mathematical Topics on Which to Practice Proof Techniques ............ 71</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Basic Set Theory and Indexed Families ....................................... 71</td>
</tr>
<tr>
<td></td>
<td>Cartesian Product of Sets ................................................................ 82</td>
</tr>
<tr>
<td></td>
<td>Indexed Families of Sets ................................................................ 84</td>
</tr>
<tr>
<td></td>
<td>About Functions ............................................................................. 87</td>
</tr>
<tr>
<td></td>
<td>Composition of Functions ................................................................ 93</td>
</tr>
<tr>
<td></td>
<td>A Little More about Functions and Sets ......................................... 98</td>
</tr>
<tr>
<td></td>
<td>Relations ...................................................................................... 102</td>
</tr>
<tr>
<td></td>
<td>Most Common Properties of Relations .......................................... 105</td>
</tr>
<tr>
<td></td>
<td>More about Equivalence Relations ................................................ 109</td>
</tr>
<tr>
<td></td>
<td>A Special Relation and More Facts about Equivalence Classes ........ 111</td>
</tr>
<tr>
<td></td>
<td>The Basics of Groups .................................................................... 118</td>
</tr>
<tr>
<td></td>
<td>Some Properties of Binary Operations .......................................... 121</td>
</tr>
<tr>
<td></td>
<td>Special Elements .......................................................................... 128</td>
</tr>
<tr>
<td></td>
<td>When the Properties Fit Together ................................................ 131</td>
</tr>
<tr>
<td></td>
<td>Sizes and Structures ..................................................................... 138</td>
</tr>
</tbody>
</table>
Groups (mod m) and Arithmetic (mod m) .......................................................... 142
Permutations and Symmetric Groups ............................................................... 148
Isomorphism and Subgroups ........................................................................... 152
An Important Theorem .................................................................................. 156
Limits ............................................................................................................. 159
Getting Closer ............................................................................................... 162
Functions and Limits ...................................................................................... 169
Sizes of Infinity ............................................................................................... 179

CHAPTER 5 Review Exercises ............................................................................. 189
Exercises without Solutions ............................................................................ 192
General Topics ................................................................................................ 192
Basic Set Theory .............................................................................................. 195
About Functions .............................................................................................. 196
Relations .......................................................................................................... 196
The Basics of Groups ...................................................................................... 197
Limits ................................................................................................................. 197
Cardinality and Sizes of Infinity ...................................................................... 198
Collection of “Proofs” ..................................................................................... 198
Solutions for the Exercises at the End of the Sections and the Review Exercises .................................................................................. 204
Solutions for the Exercises at the End of the Sections .................................... 204
Chapter 2: Basic Techniques to Prove If/Then Statements .......................... 204
Chapter 3: Special Kinds of Theorems ............................................................. 210
Chapter 4: Some Mathematical Topics on Which to Practice Proof Techniques ............................................................................................... 225
Solutions for the Review Exercises .................................................................. 258
Other Books on the Subject of Proofs and Mathematical Writing .................. 278

Index ................................................................................................................. 281
List of Symbols

Natural or counting numbers: \( \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\} \)
Prime numbers = \{2, 3, 5, 7, 11, 13, \ldots\}
Whole numbers = \( \mathbb{W} = \{0, 1, 2, 3, 4, 5, \ldots\}\)
Integer numbers = \( \mathbb{Z} = \{\ldots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}\)
Rational numbers = \( \mathbb{Q} = \{\text{numbers of the form } \frac{a}{b} \text{ with } a \text{ and } b \text{ integers and } b \neq 0\}\)
Irrational numbers = \{numbers that cannot be represented as the quotient of two integers\}
Real numbers = \( \mathbb{R} = \{\text{all rational and irrational numbers}\} \)
Complex numbers = \( \mathbb{C} = \{\text{numbers of the form } a + ib \text{ with } a \text{ and } b \text{ real numbers and } i \text{ such that } i^2 = -1\}\)

\( n! = n \times (n-1) \times (n-2) \times \ldots \times 3 \times 2 \times 1 \) (read “n factorial”) is defined for all \( n \geq 0 \). By definition \( 0! = 1 \).

\{x \mid x \text{ has a certain property}\} gives the description of a set. In this context the symbol “\( \mid \)” is read “such that.” All objects that have the required property are called “elements” of the set.

\( a \in A: a \) is an element of the set \( A \) (see Section on Basic Set Theory in Chapter 4)
\( a \notin A: a \) is not an element of the set \( A \) (see Section on Basic Set Theory in Chapter 4)
\( A \subseteq B: \) the set \( A \) is contained (or equal to) in the set \( B \) (see Section on Basic Set Theory in Chapter 4)
\( A \cup B: \) read “\( A \) union \( B \)” (see Section on Basic Set Theory in Chapter 4)
\( A \cap B: \) read “\( A \) intersection \( B \)” (see Section on Basic Set Theory in Chapter 4)
\( A' = C(A): \) read “complement of \( A \)” (see Section on Basic Set Theory in Chapter 4)

\( |x| = \text{absolute value of } x = \text{distance from 0 to } x = \begin{cases} x \text{ when } x \geq 0 \\ -x \text{ when } x < 0 \end{cases} \)

SOME FACTS AND PROPERTIES OF NUMBERS

Trichotomy Property of Real Numbers
Given two real numbers \( a \) and \( b \), exactly one of the following three relations holds true: 1) \( a < b \); 2) \( a = b \); 3) \( a > b \).

Selected Relations, Definitions, and Properties of Integer, Rational, and Irrational Numbers

The following definitions are given only for integer numbers:
An integer number \( a \) is divisible by a nonzero integer number \( b \) if there exists an integer number \( n \) such that \( a = bn \). The number \( a \) is said to be a multiple of \( b \), and \( b \) is said to be a divisor (or a factor) of \( a \).
Numbers that are multiples of 2 are called even. Therefore, for any even number \( a \) there exists an integer number \( k \) such that \( a = 2k \). Numbers that are not divisible by 2 are said to be odd; thus, any odd number \( t \) can be written as \( t = 2s + 1 \) for some integer number \( s \).

The following relations, definitions, and properties are given only for positive integer numbers:
A counting number larger than 1 is called prime if it is divisible only by two distinct counting numbers, itself and 1. Because of this definition, the number 1 is not a prime number.
The \( \text{lcm}(a, b) = \text{least common multiple} \) of \( a \) and \( b \), call it \( L \), is the smallest multiple that the positive integers \( a \) and \( b \) have in common. Therefore,
I. there exist two positive integers \( n \) and \( m \) such that \( L = an \) and \( L = bm \);
ii. if \( M \) is another common multiple of \( a \) and \( b \), then \( M \) is a multiple of \( L \); and
iii. \( L \geq a \) and \( L \geq b \).
The \( \text{GCD}(a, b) = \text{greatest common divisor} \) of \( a \) and \( b \), call it \( D \), is the largest divisor that the positive integers \( a \) and \( b \) have in common. Therefore,

i. there exist two positive integers \( s \) and \( t \) such that \( a = Ds \) and \( b = Dr \); with \( s \) and \( t \) relatively prime (i.e., having no common factors);

ii. if \( T \) is another common divisor of \( a \) and \( b \), then \( T \) is a divisor of \( D \); and

iii. \( D \leq a \) and \( D \leq b \).

If \( \text{GCD}(a, b) = 1 \), then \( a \) and \( b \) are said to be \textit{relatively prime}.

There are two equivalent definitions that are usually employed when dealing with \textit{rational numbers}. The first is the one given above, with rational numbers considered to be the ratio (quotient) of two integers, where the divisor is not equal to zero. When using this definition, it might be useful to remember that it is always possible to represent a rational number as a fraction whose numerator and denominator have no common factors (relatively prime) (e.g., use \( 1/3 \) instead of \( (-6)/(-18) \) or \( 3/9 \)). This kind of fraction is said to be in \textit{reduced form}.

The second definition states that a number is rational if it has either a finite decimal part OR an infinite decimal part that exhibits a repeating pattern. The repeating set of digits is called the \textit{period} of the number. It can be proved that these two definitions are equivalent.

The two definitions used for rational numbers generate two definitions for \textit{irrational numbers}. The first one is the one given above. The second states that a number is irrational if its decimal part is infinite AND does not exhibit a repeating pattern.

\textbf{Well-Ordering Principle}

Every nonempty set of nonnegative integers contains a smallest element.

\textbf{Division Algorithm}

Let \( a \) and \( b \) be two integers. Then there exist two integers \( q \) and \( r \) such that

\[ a = qb + r \]

with \( 0 \leq r < |b| \). The number \( q \) is the \textit{quotient}, the number \( r \) is the \textit{remainder}. (For a proof of this fact see the section on Existence Theorems in Chapter 3.)

\textbf{SOME FACTS AND PROPERTIES OF FUNCTIONS}

Let \( f \) and \( g \) be two real 0 valued functions. Then it is possible to construct the following functions:

1. \( f + g \) defined as \( (f + g)(x) = f(x) + g(x) \)
2. \( f - g \) defined as \( (f - g)(x) = f(x) - g(x) \)
3. \( fg \) defined as \( (fg)(x) = f(x)g(x) \)
4. \( f/g \) defined as \( (f/g)(x) = f(x)/g(x) \) when \( g(x) \neq 0 \)
5. \( fg \) defined as \( (f \circ g)(x) = f(g(x)) \)

The domains of these functions will be determined by the domains and properties of \( f \) and \( g \).

A function \( f \) is said to be

1. **Increasing** if for every two real numbers \( x_1 \) and \( x_2 \) such that \( x_1 < x_2 \), it follows that \( f(x_1) < f(x_2) \).
2. **Decreasing** if for every two real numbers \( x_1 \) and \( x_2 \) such that \( x_1 < x_2 \), it follows that 
\[
f(x_1) > f(x_2).
\]

3. **Nondecreasing** if for every two real numbers \( x_1 \) and \( x_2 \) such that \( x_1 < x_2 \), it follows that 
\[
f(x_1) \leq f(x_2).
\]

4. **Nonincreasing** if for every two real numbers \( x_1 \) and \( x_2 \) such that \( x_1 < x_2 \), it follows that 
\[
f(x_1) \geq f(x_2).
\]

5. **Odd** if \( f(-x) = -f(x) \) for all \( x \).

6. **Even** if \( f(-x) = f(x) \) for all \( x \).

7. **One-to-one** if for every two real numbers \( x_1 \) and \( x_2 \) such that \( x_1 \neq x_2 \), it follows that \( f(x_1) \neq f(x_2) \).

8. **Onto** if for every value \( y \) there is at least one value \( x \) such that \( f(x) = y \).