Introduction

- Formal proofs of theorems designed for human consumption are almost always informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated.

Some Terminology

<table>
<thead>
<tr>
<th>Table 1. Terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Term</strong></td>
</tr>
<tr>
<td>Theorem</td>
</tr>
<tr>
<td>Proposition</td>
</tr>
<tr>
<td>Proof</td>
</tr>
<tr>
<td>Fact</td>
</tr>
<tr>
<td>Result</td>
</tr>
<tr>
<td>Axiom</td>
</tr>
<tr>
<td>Postulate</td>
</tr>
<tr>
<td>Lemma</td>
</tr>
<tr>
<td>Corollary</td>
</tr>
<tr>
<td>Conjecture</td>
</tr>
</tbody>
</table>

Understanding How Theorems are Stated

EXAMPLE 0 Complete the statement below by adding the qualification.

“If $x > y$, where $x$ and $y$ are positive real numbers, then $x^2 > y^2$.”

Solution: The foregoing statement really means

“For all positive real numbers $x$ and $y$, if $x > y$, then $x^2 > y^2$.”

or

$$\forall x \forall y (P(x) \rightarrow Q(x))$$

$P(x)$  $x > y$
$Q(x)$  $x^2 > y^2$
Domain  $x, y \in \mathbb{R}$
Methods of Proving Theorems

Objective: Prove a theorem of the form $\forall x (P(x) \rightarrow Q(x))$

Solution:
1. Show $P(c) \rightarrow Q(c)$
2. $c$ is an arbitrary element of the domain
3. Apply universal generalization

Direct Proofs

1. In the statement, $p \rightarrow q$, $p$ is assumed to be true.
2. Axioms, definitions, and previously proven theorems are used with rules of inference to show that $q$ must also be true.

DEFINITION 1 The integer $n$ is even if there exists an integer $k$ such that $n = 2k$, and $n$ is odd if there exists and integer $k$ such that $n = 2k + 1$. (Note that an integer is either even or odd, and no integer is both even and odd.)

EXAMPLE 1 Give a direct proof of the theorem “if $n$ is an odd integer, then $n^2$ is odd.”

Solution:
1. The theorem states: $\forall n (P(n) \rightarrow Q(n))$
2. $P(n)$: $n$ is an odd integer.
3. $Q(n)$: $n^2$ is an odd integer.
4. Assume $n$ is an arbitrarily chosen odd integer.
5. $P(n)$ is true.
6. $n = 2k + 1$, where $k$ is some integer.
7. $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
8. Let $l = 2k^2 + 2k$, then $n^2 = 2l + 1$.
9. $2l + 1$ is an odd integer by the definition and so is $n^2$

EXAMPLE 2 Give a direct proof that if $m$ and $n$ are both perfect squares, then $mn$ is also a perfect square. (An integer $a$ is a perfect square if there is an integer $b$ such that $a = b^2$.)

Solution: To produce a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that $m$ and $n$ are both perfect squares. By the definition of a perfect square, it follows that there are integers $s$ and $t$ such that $m = s^2$ and $n = t^2$. The goal of the proof is to show that $mn$ must also be a perfect square when $m$ and $n$ are: looking ahead we see how we can show this by multiplying the two equations $m = s^2$ and $n = t^2$ together. This shows that $mn = s^2t^2$, which implies that $mn = (st)^2$ (using commutivity and associativity of multiplication). By the definition of perfect square, it follows that $mn$ is also a perfect square, because it is the square of $st$, which is an integer. We have proved that if $m$ and $n$ are both perfect squares, then $mn$ is also a perfect square.
Proof by Contraposition

- Called **indirect proofs**.
- Called **proof by contraposition**.

\[ p \rightarrow q \equiv \neg q \rightarrow \neg p \]

**EXAMPLE 3**

Prove that if \( n \) is an integer and \( 3n + 2 \) is odd, then \( n \) is odd.

**Solution:**

1. Assume \( n \) is even.
2. \( n = 2k \), definition of **even**.
3. \( 3(2k) + 2 = 6k + 2 = 2(3k + 1) \)
4. \( 3n + 2 \) must be even because if \( n \) is even we have found that \( 3n + 2 \) is a multiple of 2, namely \( 2(3k + 1) \).
5. Since an integer cannot both be even and odd at the same time \( 3n + 2 \) is not odd.
6. However, the statement that \( 3n + 2 \) is not odd contradicts the hypothesis that \( 3n + 2 \) is even.
7. Therefore \( n \) must be odd.
8. We have proved the theorem “If \( 3n + 2 \) is odd, then \( n \) is odd.

Proof by Contradiction

- Called **indirect proofs**.
- Called **proof by contradiction**.

Because the proposition \( r \land \neg r \) is a contradiction whenever \( r \) is a proposition, we can prove that \( p \) is true if we can show that \( \neg p \rightarrow (r \land \neg r) \) is true for some proposition. Proofs of this type are called **proofs by contradiction**.
EXAMPLE 10  Prove $\sqrt{2}$ is irrational by giving a proof by contradiction

Solution:

Step  Argument
1  Let $p$ be the proposition “$\sqrt{2}$ is irrational.”
2  $\neg p$ is the proposition “$\sqrt{2}$ is rational.”
3  Assume $\neg p$ is true.
4  If $\sqrt{2}$ is rational, then there exist integers $a$ and $b$ with $\sqrt{2} = \frac{a}{b}$, where $b \neq 0$, and $a$ and $b$ have no common factors (so that the fraction $\frac{a}{b}$ is in lowest terms).
5  By squaring both sides of the equality $\sqrt{2} = \frac{a}{b}$, we obtain $2 = \frac{a^2}{b^2}$.
6  Hence $2b^2 = a^2$.
7  By the definition of an even integer, $a^2$ is even because it contains a factor of 2.
8  Since $a^2$ is even, $a$ must be even also.
9  Since $a$ is even, we can write $a = 2c$, for some integer $c$.
10 Recall $2b^2 = a^2$ and substitute $2c$ for $a$ arriving at the equations $2b^2 = 4c^2$.
11 We have now shown that the assumption of $\neg p$ leads to the equation $\sqrt{2} = \frac{a}{b}$, where $a$ and $b$ have no common factors, but both $a$ and $b$ are even, that is, 2 divides both $a$ and $b$. Note that the statement $\sqrt{2} = \frac{a}{b}$, where $a$ and $b$ have no common factors, means, in particular, that 2 does not divide both $a$ and $b$. Because our assumption of $\neg p$ leads to the contradiction that 2 divides both $a$ and $b$ and 2 does not divide both $a$ and $b$, $\neg p$ must be false. That is, the statement $p$, “$\sqrt{2}$ is irrational,” is true. We have proved $\sqrt{2}$ is irrational.