Unit-2
Notion of Proof

NAVRACHNA UNIVERSITY

B.TECH. CSE

SEMESTER III

A.Y. 2023-24

Introduction

- Formally, a **theorem** is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important.
- Less important theorems sometimes are called **propositions**.
- A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion.
- We demonstrate that a theorem is true with a **proof**. A proof is a valid argument that establishes the truth of a theorem.

Introduction

- The statements used in a proof can include **axioms** (or **postulates**), which are statements we assume to be true the premises, if any, of the theorem, and previously proven theorems.
- A less important theorem that is helpful in the proof of other results is called a **lemma** (plural *lemmas* or *lemmata*).
- A **corollary** is a theorem that can be established directly from a theorem that has been proved.
- A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

Direct Proof

- A direct proof shows that a conditional statement $p \to q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs.

Direct Proof

- **Definition:** The integer *n* is *even* if there exists an integer *k* such that *n* = 2*k*, and *n* is *odd* if there exists an integer *k* such that *n* = 2*k* + 1.
- **Example:** Give a direct proof of the theorem "If *n* is an odd integer, then n^2 is odd."
- ***Solution:*** Let P(n): $n\ is\ odd\ number$ and Q(n): $n^2\ is\ odd\ number$.

To prove: $\forall n, P(n) \rightarrow Q(n)$

By direct proof, if $\forall n$ P(n) is true

$\rightarrow n\ is\ odd$

$\rightarrow n = 2k + 1, where\ k \in Z$

$\rightarrow n^2 = (2k + 1)^2,\ \ squaring\ both\ sides$

$\rightarrow n = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

$\rightarrow n = 2m + 1\ ,\ where\ m(= 2k^2 + 2k) \in Z$

$\rightarrow n^2\ is\ odd \rightarrow$ Q(n) is true

Thus $\forall n, P(n) \rightarrow Q(n)$.

Exercise

- **Definition:** If a divides b then b is multiple of a, i.e. $b = ak\ (k \in Z)$.
- **Exercise:** Let a, b and c be integers, directly prove that if a divides b and a divides c then a also divides b + c.
- **Solution**: Predicate (p): a divides b and c , Conclusion (q): a divides (b+c)

  To prove $p \to q$.

  By direct proof, if p is true

  $\to a\ divides\ b\ and\ c$

  $\to b = ak, c = al, \quad (k, l \in Z)$

  $\to b + c = ak + al = a(k + l) = am, (m(= k + l) \in Z)$

  $\to a\ divides\ (b + c) \to q\ is\ true.$

  Thus $p \to q$

Exercise

- Directly prove that if m and n are odd integers then mn is also an odd integer.
- Proof: p: $m\ and\ n\ are\ odd\ numbers$, q: $mn\ is\ odd\ number$

  To prove $p \rightarrow q$

  By direct proof, if p is true

  $\rightarrow m\ and\ n\ are\ odd$

  $\rightarrow m = 2k + 1\ , n = 2l + 1,\ \ (k, l \in Z)$

  $\rightarrow mn = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$

  $\rightarrow mn = 2r + 1,\ \ (r(= 2kl + k + l) \in Z)$

  $\rightarrow mn\ is\ odd$

  $\rightarrow q\ is\ true$

  Thus $p \rightarrow q$.

Exercise

- Definition: An integer m is a perfect square if $m = k^2$ for some integer k
- Let m and n be integers. Directly prove that if m and n are perfect squares then mn is also a perfect square.
- Proof: p: $m\ and\ n\ are\ perfect\ squares$, q: $mn\ is\ also\ perfect\ squares$

  To prove $p \rightarrow q$

  By direct proof, if p is true

  $\rightarrow m\ and\ n\ are\ perfect\ squares$

  $\rightarrow m = k^2, n = l^2,\ (k, l \in Z)$

  $\rightarrow mn = k^2 l^2 = (kl)^2 = r^2, \quad (r(= (kl)^2) \in Z)$

  $\rightarrow mn\ is\ perfect\ square$

  $\rightarrow q\ is\ true$

  Thus $p \rightarrow q$.

Exercise

- Definition: The real number r is rational if there exist integers p and q with q≠0 such that r = p/q. A real number that is not rational is called irrational.
- Prove that the sum of two rational numbers is rational.
- Proof: $p: m\ and\ n\ are\ rational\ ,\quad q: (m+n)\ is\ rational$

  To prove p $\rightarrow q$

  $p: m = \frac{a}{b}\ , n = \frac{c}{d}\ \ (a, b, c, d\ \in Z, b \neq 0, d \neq 0)$ and

  $q: m + n = \frac{k}{l}\ , (k, l \in Z, l \neq 0)$

  $m + n = \frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} = \frac{k}{l}\ \ ,\quad (k = ad + cb, l = bd)$

  Here $a, b, c, d\ \in Z, b \neq 0, d \neq 0$. So, $k, l \in Z, l \neq 0$

  Hence $m + n$ is rational, i.e. q is true.

  Thus $p \rightarrow q$.

Exercise

Prove directly that

1. If n is an even integer then 7n + 4 is an even integer.
2. If m is an even integer and n is an odd integer then m + n is an odd integer.
3. If m is an even integer and n is an odd integer then mn is an even integer
4. Sum of two odd integers is even.
5. If a,b, c ∈ N, then lcm(ca, cb) = c ·lcm(a,b)
6. Let x and y be positive numbers. If x ≤ y, then $\sqrt{x} \leq \sqrt{y}$ (Prove without taking square root on both sides).

Proof by Contraposition

- Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called **indirect proofs**.
- An extremely useful type of indirect proof is known as **proof by contraposition**.
- Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$.

Exercise

- Prove that if *n* is an integer and 3*n* + 2 is odd, then *n* is odd.
- Proof: Let p: $(3n + 2) is\ odd$, q: $n\ is\ odd$

  To prove: $p \rightarrow q$ (direct proof not possible) or $\sim q \rightarrow \sim p$ (contrapositive)

  $\sim p$: $(3n + 2)\ is\ even$, $\sim q$: $n\ is\ even$

  By contrapositive proof, if $\sim q$ is true

  $\rightarrow n\ is\ even$

  $\rightarrow n = 2k \quad (k \in Z)$

  $\rightarrow 3n = 6k\ \ (multiplying\ by\ 3\ both\ sides)$

  $\rightarrow 3n + 2 = 6k + 2 \quad (adding\ 2\ both\ sides)$

  $\rightarrow 3n + 2 = 2(3k + 1) = 2r \quad (r = (3k + 1) \in Z)$

  $\rightarrow (3n + 2)\ is\ even$

  $\rightarrow \sim p\ is\ true$

  Hence $\sim q \rightarrow \sim p$ or $p \rightarrow q$.

Exercise

- Prove by contraposition that If 7x+9 is even, then x is odd.

Proof:

- Suppose x is not odd.
- Thus x is even, so x = 2a for some integer a.
- Then $7x + 9 \ = \ 7(2a) + 9 \ = \ 14a + 8 + 1 \ = \ 2(7a + 4) + 1$.
- Therefore $7x + 9 \ = \ 2b \ + 1, where\ b\ is\ the\ integer\ 7a + 4$.
- Consequently $7x + 9\ is\ odd$. Therefore $7x + 9\ is\ not\ even$.

Exercise

- Prove by contraposition that If $x^2 - 6x + 5$ is even, then x is odd.

Proof:

- Suppose $x\ is\ not\ odd$.
- Thus $x\ is\ even$, so $x = 2a$ for some integer a.
- So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5$

  $= 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1$

  $= 2(2a^2 - 6a + 2) + 1.$
- Therefore $x^2 - 6x + 5 = 2b + 1$, where b is the integer $2a^2 - 6a + 2$. Consequently $x^2 - 6x + 5$ is odd.
- Therefore $x^2 - 6x + 5$ is not even

Exercise

1. Show that by Contraposition: For any integer k, prove if 3k + 1 is even, then k is odd.
2. Show that by Contraposition: For any integers a and b, a + b ≥ 15 implies that a ≥ 8 or b ≥ 8.
3. Show that by Contraposition if n is a positive integer such that the sum of its positive divisors is n+1 then n is prime.
4. Suppose $x, y \in R$. Prove by contraposition: If $y^3 + yx^2 \leq x^3 + xy^2$, then y ≤ x.
5. Prove by contraposition: Suppose $x, y \in Z$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proofs by Contradiction

- The statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r.
- Proofs of this type are called **proofs by contradiction**.
- Start with assuming p → ~r to be true and find a contradiction to p which will lead to conclusion p →r.

Prove that $\sqrt{2}$ is irrational by giving a proof of contradiction.

Proof: Suppose that $\sqrt{2}$ is rational.

(We will show this leads to contradiction)

Then $\sqrt{2} = \frac{a}{b}$ where $a, b \in Z$ such that a and b have no common factors.

Squaring both sides, we get

$$2 = \frac{a^2}{b^2}$$

$$\rightarrow 2b^2 = a^2$$

$$\rightarrow a^2\ is\ multiple\ of\ 2\ i.e.\ a^2\ is\ even$$

$$\rightarrow a\ is\ also\ even$$

$$\rightarrow a = 2k\ , for\ some\ k \in Z$$

$$\rightarrow 2b^2 = (2k)^2$$

$$\rightarrow b^2 = 2k^2$$

$$\rightarrow b^2\ is\ even\ \ \rightarrow b\ is\ even$$

But now a and b both are even. So a and b have a common factor 2 which is contradiction to the statement a and b have no common factors.

Hence our initial assumption that $\sqrt{2}$ is rational is false. Thus $\sqrt{2}$ is irrational

Exercise

- Prove by contradiction:

1. If $x = 2$ then $3x - 5 \neq 10$.
2. If a,b,c are all odd integers, then $ax^2 + bx + c = 0$ cannot have rational solution.
3. If ΔABC then measures of each base angles cannot be $92°$.
4. If $\angle A$ & $\angle B$ are complementary then $\angle A \leq 90°$.

Proof by counter example

- A theorem can be disproved or proved as false by giving counter example.
- Converse of $p \rightarrow q$ is $q \rightarrow p$.
- This is the method of Proof by Counter example.

Exercise

- Disprove by counterexample that the product of two irrational numbers is always irrational.
- Disprove the statement given below by counterexample.

  The equation $p^4 = q^4$ is true if and only if $p = q$, where p and q are real numbers.

- Show that the statement $n^2 - n + 5$ cannot be a perfect square for any n, where n belongs to the natural numbers" is false.

Exercise

- Prove that the converse of this statement is false.

If $2^n - 1$ prime, then n is prime.

Solution

The converse statement is "If n is prime, then $2^n - 1$ is prime." But the case $n = 11$ is a ***counterexample***:

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

is not prime even though $n = 11$ is prime.

Thank you

Swapnila R. Nigam

Assistant Professor (SET),

swapnila.nigam@nuv.ac.in