Proof Techniques

Proofs

Theorem: the main result that
we want to prove

Lemma: intermediate result
used in theorem proof

Axiom: basic truth

Corollary: immediate consequence of theorem

Conjecture: something to be proven

Typically, we want to prove statements

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

Proof technique:

show that for some arbitrary c

$$P(c) \rightarrow Q(c)$$

and apply universal generalization

Direct proof: $P(c) \to Q(c)$

Proof by contraposition: $\neg Q(c) \to \neg P(c)$

Proof by contradiction: $\neg P(c) \to (r \wedge \neg r)$

If we want to prove $P(c)$

Definition: $\text{integer } n \text{ is even} \leftrightarrow \exists k\ n = 2k$

$$\text{integer } n \text{ is odd} \leftrightarrow \exists k\ n = 2k + 1$$

An integer is either even or odd

Theorem: if n is an even integer, $P(n)$

then n^2 is even $Q(n)$

Proof: (direct proof) $P(n) \rightarrow Q(n)$

$$n \text{ is even} \rightarrow \exists k \; n = 2k$$

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

Therefore, n^2 is even

End of proof

Theorem: if n is an odd integer, then n^2 is odd

$P(n)$

$Q(n)$

Proof: (direct proof) $P(n) \to Q(n)$

$$n \text{ is odd} \to \exists k \; n = 2k+1$$

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

Therefore, n^2 is odd

End of proof

Theorem: if n^2 is an even integer, $P(n)$
then n is even $Q(n)$

Proof: (proof by contraposition) $\neg Q(n) \to \neg P(n)$

$$\neg Q(n) \to \neg P(n)$$

$$n \text{ is odd} \to n^2 \text{ is odd}$$ (see last proof)

Therefore: $$P(n) \to Q(n)$$

End of proof

Theorem: if n^2 is an odd integer, $P(n)$

then n is odd $Q(n)$

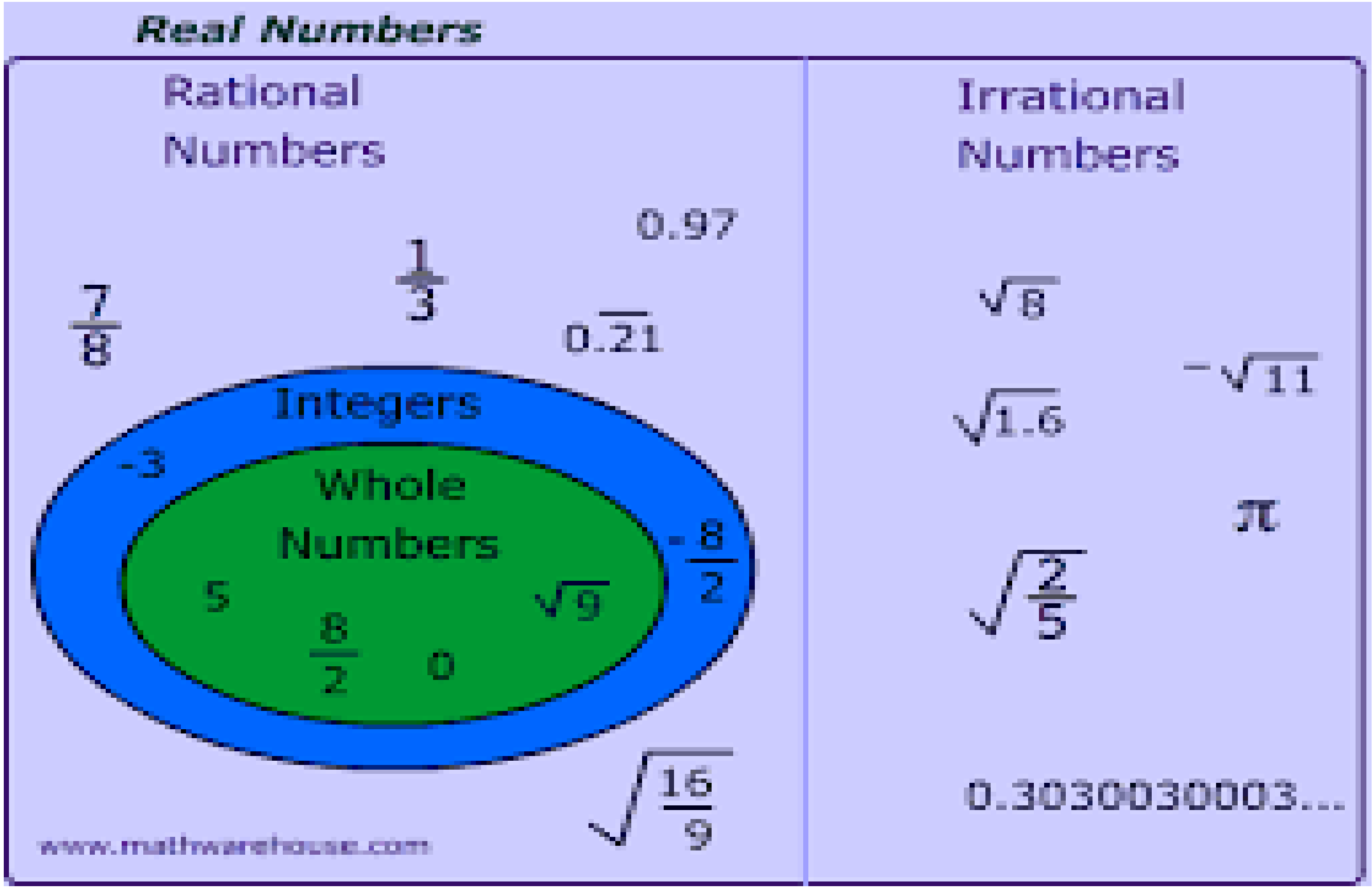
Proof: (proof by contraposition) $\neg Q(n) \to \neg P(n)$

$$\neg Q(n) \to \neg P(n)$$

$$n \text{ is even} \to n^2 \text{ is even}$$

Therefore: $P(n) \to Q(n)$

End of proof



Real Numbers
Rational Numbers
Irrational Numbers
0.97
$\frac{1}{3}$
$\frac{7}{8}$
$0.\overline{21}$
Integers
-3
Whole Numbers
5
$\frac{8}{2}$
0
$\sqrt{9}$
$-\frac{8}{2}$
$\sqrt{\frac{16}{9}}$
www.mathwarehouse.com
$\sqrt{8}$
$-\sqrt{11}$
$\sqrt{1.6}$
π
$\sqrt{\frac{2}{5}}$
0.3030030003...

Theorem: $\sqrt{2}$ is irrational P

Proof: (proof by contradiction) $\neg P \rightarrow (r \wedge \neg r)$

$\neg P:$ Assume $\sqrt{2}$ is rational

$$\sqrt{2} = \frac{m}{n}$$

$r:$ m and n have no common divisor greater than 1

Therefore: $\neg P \rightarrow r$

$$2 = \frac{m^2}{n^2} \Rightarrow m^2 = 2n^2 \Rightarrow m = 2k_1 \ (m \text{ is even})$$

$$2n^2 = m^2 = 4{k_1}^2 \Rightarrow n^2 = 2{k_1}^2 \Rightarrow n = 2k_2 \ (n \text{ is even})$$

$\neg r:$ $\frac{m}{n} = \frac{2k_1}{2k_2}$ common divisor is 2

Therefore: $\neg P \rightarrow \neg r$

Therefore:

$$\neg P \rightarrow r$$

$$\neg P \rightarrow \neg r$$

$\therefore (\neg P \rightarrow r) \wedge (\neg P \rightarrow \neg r)$ Conjunction

$\equiv \neg P \rightarrow (r \wedge \neg r)$ contradiction

Therefore:

$$\neg P \rightarrow (r \wedge \neg r)$$

$$\neg(r \wedge \neg r)$$

$$\therefore \neg(\neg P) \qquad \text{Modus Tollens}$$

$$\equiv P$$

End of proof

Counterexamples

False statement:

"Every positive integer is the sum of the squares of two integers"

$$\forall x > 0\ \exists y \exists z (x = y^2 + z^2)$$

Counterexample: $x = 3$

$$3 \neq 1^2 + 1^2 = 2$$

$$3 \neq 1^2 + 2^2 = 1 + 4 = 5$$

Any other combination gives sum larger than 3

Proof by cases

We want to prove $p \to q$

We know $p = p_1 \vee p_2 \vee \cdots \vee p_n$

Instead, we can prove each case

$$p \to q$$

$$\equiv p_1 \vee p_2 \vee \cdots \vee p_n \to q$$

$$\equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)$$

Case 1 Case 2 Case n

Theorem: If n is integer, then $n^2 \geq n$

Case 1 Case 2 Case 3

Proof: $n \text{ is integer} \equiv (\mathrm{n} = 0) \vee (\mathrm{n} \geq 1) \vee (\mathrm{n} \leq \text{-}1)$

Case 1: $\mathrm{n} = 0$ $\mathrm{n}^2 = 0^2 = 0 = n$

Case 2: $\mathrm{n} \geq 1$ $n^2 = n \cdot n \geq n \cdot 1 = n$

Case 3: $\mathrm{n} \leq -1$ $n^2 > 0 > n$

End of proof

Existence Proofs

Theorem: There is a positive integer that can be written as the sum of cubes in two different ways

Proof: (constructive existence proof)

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

End of proof

Theorem: There exist irrational numbers x, y such that x^y is rational

Proof: (non-constructive existence proof)

We know: $\sqrt{2}$ is irrational

If $\sqrt{2}^{\sqrt{2}}$ is rational $\Rightarrow$ $x = \sqrt{2}, \quad y = \sqrt{2}$

If $\sqrt{2}^{\sqrt{2}}$ is irrational $\Rightarrow$ $x = \sqrt{2}^{\sqrt{2}}, \quad y = \sqrt{2}$

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{2} = 2 = \frac{2}{1}$$ rational

End of proof