EX. HYPOTHESES: $\exists x\,(P(x) \wedge \neg Q(x))$
$\forall x\,(P(x) \to R(x))$
CONCLUSION: $\exists x\,(R(x) \wedge \neg Q(x))$

1.)	$\exists x\,(P(x) \wedge \neg Q(x))$	HYPOTHESIS
2.)	$\forall x\,(P(x) \to R(x))$	HYPOTHESIS
3.)	$P(a) \wedge \neg Q(a)$	EXIST. INST. 1
4.)	$P(a)$	SIMP. 3
5.)	$P(a) \to R(a)$	UNIV. INST. 2
6.)	$R(a)$	MODUS PONENS 4,5
7.)	$\neg Q(a)$	SIMP. 3
8.)	$R(a) \wedge \neg Q(a)$	CONJUNCTION 6,7
9.)	$\exists x\,(R(x) \wedge \neg Q(x))$	EXIST. GEN 8

NOTE: SCOPE OF QUANTIFIERS

$$\forall x\,(P(x) \to Q(x)) \not\equiv \forall x\,P(x) \to \forall x\,Q(x)$$

EX. $U = \{$ALL PEOPLE$\}$
$P(x) =$ ' x HAS GREEN EYES'
$Q(x) =$ ' x is 50 FEET TALL'

$\forall x\,(P(x) \to Q(x))$ is FALSE
$\forall x\,P(x) \to \forall x\,Q(x)$ is TRUE (WHY?)

IN ORDER TO ILLUSTRATE SOME METHODS OF PROOF WE FIRST MAKE A FEW DEFINITIONS CONCERNING THE INTEGERS. WE DENOTE BY $\mathbb{Z}$ THE SET OF INTEGERS

GIVEN $a, b \in \mathbb{Z}$ WITH $a \neq 0$, WE SAY a <u>DIVIDES</u> b IFF $b = ak$ FOR SOME $k \in \mathbb{Z}$. NOTATION: $a \mid b$.

n IS CALLED <u>EVEN</u> IF $2 \mid n$, AND <u>ODD</u> OTHERWISE. THUS n IS EVEN IFF $\exists k : n = 2k$ AND n IS ODD IFF $\exists k : n = 2k+1$.

<u>DIRECT PROOF OF $p \to q$</u>

ASSUME p IS TRUE THEN USE VALID RULES OF INFERENCE AND PREVIOUSLY PROVED THEOREMS TO SHOW q IS TRUE.

<u>EX.</u> IF n IS ODD THEN n^2 IS ODD.

<u>PROOF:</u>

ASSUME n IS ODD. THEN $n = 2k+1$ FOR SOME INTEGER k. THUS $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. SINCE $2k^2 + 2k$ IS ITSELF AN INTEGER, THIS SHOWS n^2 IS ALSO ODD, AS CLAIMED.

///

INDIRECT PROOF. OF $P \to q$

PROVE THE CONTRAPOSITIVE STATEMENT $\neg q \to \neg P$, USUALLY DIRECTLY.

EX. IF $5n+4$ IS ODD THEN n IS ODD.

PROOF

ASSUME n IS EVEN. THEN $n = 2k$ FOR SOME INTEGER k. THUS $5n+4 = 5(2k)+4 = 2(5k+2)$. SINCE $5k+2$ IS ITSELF AN INTEGER, THIS SHOWS $5n+4$ IS ALSO EVEN. WE'VE SHOWN THAT IF n IS EVEN THEN $5n+4$ IS EVEN. HENCE IF $5n+4$ IS ODD, THEN n MUST BE ODD.

///

A REAL NUMBER x IS CALLED RATIONAL IF $x = a/b$ WHERE $a, b \in \mathbb{Z}$, $b \neq 0$. A REAL NUMBER WHICH IS NOT RATIONAL IS CALLED IRRATIONAL

LET $\mathbb{R}$ DENOTE THE SET OF REAL NUMBERS, $\mathbb{Q}$ THE SET OF RATIONAL NUMBERS, AND $\mathbb{R} - \mathbb{Q}$ THE SET OF IRRATIONAL NUMBERS.

PROOF BY CONTRADICTION OF P

PROVE THE IMPLICATION $\neg P \Rightarrow q$ WHERE q IS SOME CONTRADICTION. SINCE q IS NECESSARILY FALSE, THE ONLY WAY $\neg P \Rightarrow q$ COULD BE TRUE IS IF $\neg P$ WERE FALSE, i.e. P IS TRUE. OFTEN THE CONTRADICTION q IS OF THE FORM $q = r \wedge \neg r$ FOR SOME PROPOSITION r.

EX. $\sqrt{2}$ IS IRRATIONAL.

PROOF:

ASSUME THAT $\sqrt{2}$ IS RATIONAL. THEN THERE EXIST $a, b \in \mathbb{Z}$, $b \neq 0$ SUCH THAT

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

NOW IF a AND b HAVE ANY COMMON FACTORS WE MAY CANCEL THEM TOP AND BOTTOM. THUS WE MAY ASSUME a AND b HAVE NO FACTORS IN COMMON TO BEGIN WITH.

THUS $2 = \frac{a^2}{b^2}$, $a^2 = 2b^2$, AND a^2 IS EVEN. THIS IMPLIES a IS EVEN. (RECALL WE SHOWED n ODD $\Rightarrow n^2$ ODD WHICH PROVES INDIRECTLY THAT n^2 even $\Rightarrow n$ even.)

THUS $a = 2k$ FOR SOME $k \in \mathbb{Z}$, AND HENCE $2b^2 = a^2 = (2k)^2 = 4k^2$, $b^2 = 2k^2$. THEREFORE b^2 IS EVEN AND SO b IS EVEN.

NOW WE HAVE THAT a AND b HAVE NO COMMON FACTORS, AND YET THEY ARE BOTH EVEN. THIS CONTRADICTION SHOWS THAT OUR ORIGINAL ASSUMPTION WAS FALSE, i.e. $\sqrt{2}$ MUST BE IRRATIONAL.

///

READ · VACUOUS AND TRIVIAL PROOFS P. 64
· PROOF BY CASES P. 67

OFTEN WE WISH TO PROVE A PROPOSITION OF THE FORM $\exists x\, P(x)$ WHERE $P(x)$ IS SOME PROPOSITIONAL FUNCTION. THESE ARE CALLED <u>EXISTENCE PROOFS</u>.

<u>CONSTRUCTIVE EXISTENCE PROOF.</u>
FIND, CONSTRUCT, OR DISPLAY AN ELEMENT a IN THE UNIVERSE FOR WHICH $P(a)$ IS TRUE.

<u>NON-CONSTRUCTIVE EXISTENCE PROOF.</u>
USUALLY PROCEEDS BY CONTRADICTION.

EX. THERE EXIST IRRATIONAL NUMBERS x AND y SUCH THAT x^y IS RATIONAL

PROOF:
EITHER $\sqrt{2}^{\sqrt{2}}$ IS RATIONAL OR IT IS NOT.
IF IT IS WE ARE DONE FOR THEN $x = \sqrt{2}$, $y = \sqrt{2}$ ARE IRRATIONAL WHILE x^y IS RATIONAL.

IF $\sqrt{2}^{\sqrt{2}}$ IS IRRATIONAL TAKE $x = \sqrt{2}^{\sqrt{2}}$ AND $y = \sqrt{2}$. AGAIN WE HAVE x, y IRRATIONAL WITH

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2$$

WHICH IS RATIONAL. ///.

NOTE WE NEVER PRODUCED A PAIR x, y WITH x, y IRRATIONAL AND x^y RATIONAL. THIS IS A NON-CONSTRUCTIVE EXISTENCE PROOF.

READ: MISTAKES IN PROOFS P. 71

(1.6) SETS

DEFN

A SET is ANY (UNORDERED) COLLECTION OF OBJECTS. THE OBJECTS BELONGING TO A SET ARE CALLED IT'S MEMBERS OR ELEMENTS

THIS INTUITIVELY OBVIOUS DEFINITION LEADS DIRECTLY TO A PARADOX. SEE PROBLEM 30, P.86.

WRITE $x \in S$ TO SAY x IS A MEMBER OF SET S.

WE CAN SPECIFY A SET BY LISTING ITS MEMBERS BETWEEN BRACES $\{\ldots\}$:

$$\{1,2,3\},\ \{1,2,3,\ldots,10\},\ \{1,2,3,\ldots\}$$

SOME IMPORTANT SETS:

$\mathbb{N} = \{0,1,2,\ldots\}$ NATURAL NUMBERS
$\mathbb{Z} = \{\ldots -2,-1,0,1,2,\ldots\}$ INTEGERS
$\mathbb{Z}^+ = \{1,2,3,\ldots\}$ POSITIVE INTEGERS.
$\mathbb{Q} = \{$RATIONAL NUMBERS$\}$
$\mathbb{R} = \{$REAL NUMBERS$\}$
$\mathbb{C} = \{$COMPLEX NUMBERS$\}$

TWO SETS ARE CONSIDERED EQUAL IF THEY CONTAIN THE SAME MEMBERS. ORDER AND REPETITION IN THE LISTING ARE IRRELEVANT.

$$\{1,2,3\} = \{3,1,2\} = \{1,1,2,3,3,3\}.$$

WE CAN ALSO SPECIFY A SET USING <u>SET BUILDER NOTATION</u>. LET $P(x)$ BE A PROPOSITIONAL FUNCTION WITH UNIVERSE $\mathcal{U}$. THE SET OF ALL $x \in \mathcal{U}$ SUCH THAT $P(x)$ IS TRUE IS DENOTED

$$\{x \in \mathcal{U} \mid P(x)\}$$

OR

$$\{x \mid P(x)\}$$

IF THE UNIVERSE IS UNDERSTOOD.

$$\{x \in \mathbb{R} \mid x \leq 8\}$$

$$\{x \in \mathbb{Z} \mid x \leq 8\}$$

$$\mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n > 0\}$$

$$\mathbb{Q} = \{x \in \mathbb{R} \mid \exists a, b \in \mathbb{Z} : b \neq 0 \wedge x = \frac{a}{b}\}$$

DEFN: THE EMPTY SET IS THE SET WITH NO MEMBERS: $\phi = \{\}$.

DEFN:
WE SAY A IS A SUBSET OF B IF EVERY ELEMENT OF A IS ALSO AN ELEMENT OF B.

$$\forall x \ (x \in A \rightarrow x \in B)$$

NOTATION: $A \subseteq B$

WE SAY A IS A PROPER SUBSET OF B IF $A \subseteq B$ BUT $A \neq B$.

NOTATION: $A \subsetneq B$

RMK: $\subseteq$, $\subsetneq$, vs. $\subset$

OBSERVE THAT FOR ANY SET S:

$\phi \subseteq S$: $\forall x (x \in \phi \rightarrow x \in S)$ $F \rightarrow P$ IS TAUTOLOGY

AND

$S \subseteq S$: $\forall x (x \in S \rightarrow x \in S)$ $P \rightarrow P$ IS TAUTOLOGY

RMK: 'CONTAINS'

Ex. $S = \{1, 2\}$

The subsets of S are

$$\phi, \{1\}, \{2\}, S$$

The set of subsets of S is

$$\{\phi, \{1\}, \{1\}, S\}$$

Defn:

The set of all subsets of S is called the power set of S, and is denoted $\mathbb{P}(S)$.

Defn:

If S has n distinct members ($n \in \mathbb{N}$) we say S is finite, and that n is the cardinality of S.

Notation: $|S| = n$

If S is not finite it is called infinite.

Ex. $\mathbb{N}, \mathbb{Z}^{+}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are infinite sets.