$$\forall x(Proof(x) \rightarrow In(x, pudding))$$

"THERE is a common impression that everything that we believe ought to be capable of proof" -Bertrand Russell.

Now that we know how to write statements in the language of logic, the next issue is to prove things in this language.

1. New definitions
   (a) axiom (or postulate) is a statement we assume to be true. "For every point P and every point Q not equal to P there exists a unique line that passes through P and Q." - Euclid
   (b) A theorem is any statement proved from axioms.
   (c) Rules of Inference are the rules we use to prove things. Note that these are assumed to be true in the same way that axioms are assumed to be true.
   (d) We assume particular axioms based on our problem, but the rules or inference are pretty much agreed upon by everyone.
   (e) An argument is valid if, when the axioms are true, then the theorems are true.
2. 2 kinds of rules of inference, those that we use to infer things are true or false, and those that we use to modify our statements so that we can apply the first kind.
   (a) We normally list all our statements in a column.
   (b) Thus there is an implicit $\wedge$ between each of these. Therefore, $p \wedge q$ can be split up into p and q. Simplification or and-elimination.
   (c) No matter what p and q are, if p is true, $p \vee q$ is true. Addition or or-introduction.
   (d) The basic rule is p and $p \rightarrow q$ means we can conclude q. Modus Ponendo Ponens.
   (e) Another handy one is $\neg q$ plus $p \rightarrow q$ is $\neg p$. Modus Tollendo Tollens.
   (f) $p \rightarrow q$ plus $q \rightarrow r$ is $p \rightarrow r$. Hypothetical Syllogism.
   (g) Can we prove everything with any one of these?
   (h) What about $p \rightarrow q$ $\neg p \rightarrow q$, can't we conclude q?
   (i) $p \vee q$ plus $\neg p$, we conclude q. Modus Tollendo Ponens.
   (j) $p \vee q$ plus $\neg p \vee r$, we conclude $r \vee q$. General Resolution. With this one, we can prove everything.

(k) see http://www.informatik.htw-dresden.de/~logic/conclusions/rules.html for more about the rules.

3. That covers propositions, but what about predicates? There are a couple of extra rules we need for that.

   (a) Skolemization (book calls it Existential Instantiation). We can make up a constant and replace the variable with that constant. $\exists x(P(x) \wedge Q(x))$ becomes $P(c) \wedge Q(c)$. We do this so that we can apply...

   (b) Unification. Unification is the process of substituting a constant in for a variable when applying a rule of inference: $\forall x(P(x) \rightarrow Q(x))$ can be combined with $P(c)$ using the Unification x/c to yield $Q(c)$.

   (c) Full example: All CS majors take Networks or Databases. Midshipman Beeblebrox is a CS major who does not take Networks. Prove that Midshipman Beeblebrox takes Databases.

$$\forall x(CSMajor(x) \rightarrow Takes(x, Networks) \vee Takes(x, Databases)) \tag{1}$$
$$CSMajor(Beeblebrox) \tag{2}$$
$$\neg Takes(Beeblebrox, Networks) \tag{3}$$
$$Takes(Beeblebrox, Networks) \vee Takes(Beeblebrox, Databases)(1\&2) \tag{4}$$
$$Takes(Beeblebrox, Databases)(3\&4) \tag{5}$$

4. Now that you know what you can do in a proof, how do you know what you *should* do?

5. There are a number of different proof strategies.

   (a) Direct. Combine rules and statements just as in the example above.

   (b) proving a rule: We have some form of the type $p \rightarrow q$. We can actually do this with truth tables. Whenever p is false, the implication is true, so we don't worry about it. What we need to do is show that when p is true, q must also be true.

   If an integer n is even, then $3n$ is even:

$$\text{assume that } n \text{ really is even} \tag{6}$$
$$n = 2k \text{because any even number has two as a factor.} \tag{7}$$
$$3n = 3(2k) \tag{8}$$
$$= 2(3k) \tag{9}$$
$$\tag{10}$$

   Since $3n$ has 2 as a factor, it must be even. Since we used the assumption that n was even, we have shown that if an integer n is even, then $3n$ is even.

   (c) Indirect. When trying to prove an implication $p \rightarrow q$, assume $\neg q$ and try to show $\neg q \rightarrow \neg p$, the contrapositive. If $3n + 2$ is odd, then n is odd. Assume n is even. Then $n = 2k$ for some k. Then $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$, which is even $(\neg p)$.

(d) Contradiction. Assume the opposite of what you want to prove, and then show that this leads to a contradiction. Automatic theorem provers (mostly) all use General Resolution + Unification + Contradiction. Typically what happens is you end up with a statement p, as well as a statement $\neg p$. $p \wedge \neg p$ is a contradiction, it is always false, no matter what p is. Therefore, the opposite of what you want to prove is not valid, and thus the thing we want to prove is proven. So to prove that the sum of a rational number and an irrational number is irrational we:

$$\text{Assume its opposite: the sum of a rational and irrational number is rational} \tag{11}$$

$$j + r = s, \text{where j is irrational and r and s are rational} \tag{12}$$

$$j + \frac{a}{b} = \frac{c}{d}, \text{by definition of rational, a,b,c,d are integers} \tag{13}$$

$$j = \frac{c}{d} - \frac{a}{b} \tag{14}$$

$$j = \frac{cb - ad}{bd} \tag{15}$$

$$j = \frac{e}{f} \text{where e and f are integers} \tag{16}$$

$$j \text{ is rational since it can be expressed as ratio of integers} \tag{17}$$

$$\begin{aligned}&\text{We assumed j is irrrational, therefore we have a contradiction}\\&\text{and thus the sum of a rational and irrational must be irrational}\end{aligned} \tag{18}$$

(e) Cases. If you have something to prove of the form: $(p_1 \vee p_2 \vee p_3 \vee ... \vee p_n) \rightarrow q$, then you can break it up into $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge ... \wedge (p_n \rightarrow q)$. Then just prove each of the cases. For example, lets prove the triangle inequality, $|x| + |y| \geq |x + y|$. We this break into 3 parts: when both are ≥ 0:

$$|x| = x \tag{19}$$

$$|y| = y \tag{20}$$

$$x + y \text{ is positive, so,}$$

$$x + y = |x + y| \text{ and by substitution,} \tag{21}$$

$$\therefore |x| + |y| = |x + y|_{\square} \tag{22}$$

When both $x, y < 0$:

$$|x| = -x \tag{23}$$

$$|y| = -y \tag{24}$$

$$-x + (-y) = |x| + |y| \tag{25}$$

$$-(x + y) = |x| + |y| \tag{26}$$

$$\text{Since } x + y < 0,$$

$$-(x + y) = |x + y| \tag{27}$$

$$\therefore |x| + |y| = |x + y|_{\square} \tag{28}$$

When one (x) is ≥ 0, and the other $(y) < 0$:

$$|x| = x \tag{29}$$
$$|y| = -y \tag{30}$$
$$|x| + |y| = x + (-y) \tag{31}$$

In this 3rd case, we need to reason by cases again: If $x \geq -y$:

$$|x + y| = x + y \tag{32}$$
$$-y > y, \text{ since} y < 0 \tag{33}$$
$$x + (-y) > x + y \tag{34}$$
$$|x| + |y| > |x + y|_{\square} \tag{35}$$

If $x < y$:

$$|x + y| = -(x + y) \tag{36}$$
$$= -x + (-y) \tag{37}$$
$$x > -x \tag{38}$$
$$\therefore x + (-y) > -x + (-y)_{\square} \tag{39}$$

6. Some proof techniques relate specificly to quantifier issues, Such as existence, and uniqueness.

   (a) Existence proofs- proove $\exists x(P(x))$. The basic way is to find the example. Sometimes we can prove somethings exists without identifying it.

7. You are responsible for reading section 3.1 in your text.