More Logic Discussion

First let me apologize for stumbling over some of the ways I wanted you to do things, but it’s because I do want us to stick as closely as we can to the true definition of proof so that we know the answer to the lament:

“I know it’s true, I just don’t know how to explain it (i.e. prove it)”

Summary of what a proof of a theorem is: a numbered list of propositions, each line with a Justification. Justifications must be one of the following:

1. an Axiom or Definition or previously proven theorem. These include the basic tautologies
2. we can make an “assumption” on a line as a justification, but once we do that line and upcoming lines must be indented until the assumption is cleared out. The indentation is lost when the assumption cleared out by one of the few augmented proof techniques. The indented lines cannot be referred to later in the proof (because they are not theorems).
3. we have the Direct Proof of $P \rightarrow Q$ technique which I will call $\rightarrow$-Introduction (a technique for clearing out an indentation). Assume $P$, prove $Q$, next line is $P \rightarrow Q$.
4. we have the Proof by Exhaustion or by Cases technique (which is really a special version of the previous rule). i.e. we prove that there are some fixed number of “cases” by proving “$P_1 \lor P_2 \lor P_3$” (for example), and then we prove each of $P_i \rightarrow Q$ by having lines documented as “Case $P_i$” which is basically to assume $P_i$ at the start of a direct proof of $P_i \rightarrow Q$, and once all cases are proven, we conclude $Q$ is Proven by cases. Each of the Cases is indented, then the collection of indented Cases is cleared out on a line with $Q$ by invoking Proof by Cases.
5. We regularly use MP: if we have line i with expression $P$ and a line j with expression $P \rightarrow Q$, then a line can have $Q$ with justification “i,j, MP”. We also allow to omit explicitly having line j in the list if $P \rightarrow Q$ is a tautology or well-known previously proven theorem or axiom, and simply just mention that in the justification rather than the “j”.
6. Leibniz (substitution if you prefer). If we have proven $P \equiv Q$ on line i (or if we have two quantities $x,y$ previously proven to be equal, i.e. $x = y$), and we have line j with an expression $E[P]$ (i.e. $P$ occurring in some expression; or $E[x]$ in the latter case), then the new line can be $E[Q]$ (or $E[y]$) with justification i,j, Leibniz. Again either line i or line j can instead by a previously proven theorem or tautology etc. as a short cut.

Sample outline for using MP and Leibniz

1. ????
2. ????

... 

i. $P$  $J_i$ (justification)

i+1. $B \equiv (C \land D)$ (somehow it’s here)

j. $P \rightarrow Q$  $J_j$

k. $Q$  by i,j, MP.

k+1. $(\neg A \lor B) \equiv (A \rightarrow B)$  tautology

k+2. $(\neg A \lor (C \land D)) \equiv (A \rightarrow B)$  i+1,k+1, Leibniz
Example 2 will be a proof of Line 10 below:

1. \((\text{indent}) \, x^2 - 1 = y + 2 \) Assumption (start of a direct proof of \(\rightarrow\))
2. \(y = k - 1\) Assumption (further indented)
3. \(y + 2 = y + 2\) an \(\sim\) axiom
4. \(y + 2 = (k - 1) + 2\) 2, 3, Leibniz (right?)
5. \((x^2 - 1 = y + 2) \land (y + 2 = (k - 1) + 2)\) 1, 4 \(\land\)-introd.
6. \(x^2 - 1 = (k - 1) + 2\) 5, Trans. Axiom of \(\equiv\), MP
7. \(x^2 = k + 2\) 6, Arithm (Axiom); Leibniz

on previous line I mean that we could have done the steps necessary to “add 1 to both sides” as we’ll see more of later.

8. \(y = k - 1 \rightarrow (x^2 = k + 2)\) 2-7, \(\sim\)-Intro.
9. \((x^2 - 1 = y + 2) \rightarrow ((y = k - 1) \rightarrow (x^2 = k + 2))\) 1-8, \(\sim\)-Intro.
10. \((x^2 - 1 = y + 2) \land (y = k - 1) \rightarrow (x^2 = k + 2)\) 9, \([P \land Q \rightarrow R] \equiv [P \rightarrow (Q \rightarrow R)]\) Taut, Leibniz

Of course, there’s a simpler proof:

1. \([(x^2 - 1 = y + 2) \land (y + 2 = k + 1)] \rightarrow (x^2 - 1 = k + 1)\) Trans. \(\equiv\)-Axiom
2. \([(x^2 - 1 = y + 2) \land (y = k - 1)] \rightarrow (x^2 - 1 = k + 1)\) 1, Axiom, Leibniz
   i.e. using \((y + 2 = k + 1) \equiv (y = k - 1)\) an Arith. “Axiom”
3. \([(x^2 - 1 = y + 2) \land (y = k - 1)] \rightarrow (x^2 = k + 2)\) 2, Leibniz with Arith Axiom

What’s the “real” proof of \((x = y) \equiv (x + 2 = y + 2)?\) Well, we accept the following four equality axioms: (1) \(x = x\); (2) \((x = y) \equiv (y = x)\); (3) \([x = y] \land (y = z) \rightarrow (x = z)\); and Substitution or Leibniz (4) \((x = y) \rightarrow (E[x] \equiv E[y])\) for any expression \(E\) (and just like with tautologies the variables \(x, y\) can be replaced by any expressions that refer to values in the universe).

Then remember the two-part proof technique for biconditionals. That is, in general to prove that \(P \equiv Q\), it is enough to prove both \(P \rightarrow Q\) and \(Q \rightarrow P\) (because of a simple tautology).

We don’t even have to prove \((x = y) \rightarrow (x + 2 = y + 2)\) because it is literally an instance of \(\equiv\)-Axiom (4).

And we can prove \((x + 2 = y + 2) \rightarrow (x = y)\) as follows:

1. \(x + 2 = y + 2\) Assume
2. \((x + 2 = y + 2) \rightarrow ((x + 2) - 2 = (y + 2) - 2)\) \(\equiv\)-Axiom (4)
3. \((x + 2 - 2) = (y + 2 - 2)\) 1, 2, MP (and Assoc. Axiom)
4. \(x = y\) Arithm. Axiom; Leibniz
5. \((x + 2 = y + 2) \rightarrow (x = y)\) 1-4, \(\sim\)-intro.

Let’s make clear that the \(\land\)-introduction technique is really just a shortcut, not a new rule. Any time you use it, you are just skipping the steps from this proof:

1. \(A\) however it got here as a theorem
2. \(B\) however it got here
3. \((A \land B) \rightarrow (A \land B)\) \(\land\)-Intro
4. \(\neg(A \land B) \lor (A \land B)\) 3, taut., Leibniz
5. \(\neg A \lor \neg B \lor (A \land B)\) 4, taut., Leibniz
6. \(\neg A \lor (\neg B \lor (A \land B))\) 5, Assoc Taut., Leibniz
7. \(~A \lor (B \rightarrow (A \land B))\) 6, taut., Leibniz
8. \(A \rightarrow (B \rightarrow (A \land B))\) 7, taut., Leibniz
9. \(B \rightarrow (A \land B)\) 1,8, MP
10. \(A \land B\) 2, 9, MP

Next is a nice example of needing a proof by contraposition (i.e. instead of proving \(P \rightarrow Q\), we prove the equivalent form \(\neg Q \rightarrow \neg P\)).
Prove that \((x \neq 3) \rightarrow (4x \neq 12)\).

1. \(4x = 12\) Assume.
2. \(\frac{1}{4}(4x) = \frac{1}{4}(12)\) 1, \(\Rightarrow\)-Axiom (4), MP
3. \(x = 3\) 2, Arith. Axiom; Leibniz
4. \((4x = 12) \rightarrow (x = 3)\) 1-3, \(\rightarrow\)-Introd.
5. \((x \neq 3) \rightarrow (4x \neq 12)\) 4, taut., Leibniz

Quantifiers

Now, here are the real axioms for quantifiers (with names like (EI) for exists introd.; (AI) for forall introd.; (EE) for Exists eliminate; (AE) for forall eliminate;

(EE) if \(x\) does not occur (freely) in \(Q\) nor in any assumptions, and if you have proven \((P \rightarrow Q)\), then you can infer \((\exists x P) \rightarrow Q\)

and we can think of this as the definition of \(\forall\) in terms of \(\exists\) \((\forall x P) \equiv \sim(\exists x \sim P)\)

From the above axioms we can prove the following theorems (but we’ll treat them as axioms)

\((AE)\) \((\forall x P) \rightarrow P[x; t]\)

and we have

\((AI)\) If \(x\) does not occur in \(Q\) nor in any assumptions, and if you have proven \((Q \rightarrow P)\) then you can infer \(Q \rightarrow (\forall x P)\)

As a special case of \((AI)\), if there is no \(Q\), we have that if you can prove \(P\) and \(x\) not in any assumptions, then you can infer \((\forall x P)\). We’ll just call this \((AI)\) as well.

Axiom EI is quite clear, if you have one, then there exists one. EE is more subtle, it is not an axiom, but rather an inference rule like MP. As we discussed, if you can prove that \(Q\) holds by assuming that \(P\) holds for an \(x\) with no other assumptions on \(x\), then you can deduce that \(Q\) holds so long as \(\exists x P\). It is also essential that \(x\) does not occur (freely) in \(Q\).

Set up such a proof like this:

1. \(P\) Assume (or use \(P[x; v]\) for a fresh \(v\))
2. some steps in a proof
3. ditto
4. \(\ldots\)
7. \(Q\) Justify it (this is the one we wanted)
8. \(P \rightarrow Q\) 1-7, \(\rightarrow\)-Introd.
8. \((\exists x P) \rightarrow Q\) 8, EE

Similarly to prove \(\forall x P\) using \((AI)\).

1. \(Q\) Some assumption(s)
2. lots of lines of proof
3. ditto
4. \(P\)
5. \(Q \rightarrow P\) 1-4, \(\rightarrow\)-introd.
6. \(Q \rightarrow (\forall x P)\) 5, \(\forall\) and \(x\) is “fresh”
Here are a couple of classic statements. Let’s decide which ones are valid (meaning always true) by intuition, and then prove the ones that are valid.

1. \[ (\forall x (P(x) \to Q(x))) \land (\forall x (Q(x) \to R(x))) \to \forall x (P(x) \to R(x)) \]
2. \[ (\exists x P(x)) \land \forall x (P(x) \to Q(x)) \to \forall x Q(x) \]
3. \[ (\forall x P(x)) \land \exists x (P(x) \to Q(x)) \to \exists x Q(x) \]

1. is pretty clearly true. 2. is not: for example universe of people. Let P(x) say that x is rich, Q(x) say that x has a big house; so \((\exists x P(x))\) says there is a rich man (true); \((\forall x (P(x) \to Q(x)))\) says “everyone who is rich will have a big house” (translating math to English requires rephrasing) and we can pretend that this is true. and of course \(\forall x Q(x)\) says, wrongly, that everyone has a big house.

3. says if everything has property P and if there is someone(thing) for which having P means also having Q, then there is someone with Q. This is TRUE. The only implicit assumption (and it is always made) is that the EMPTY UNIVERSE is not allowed.

Proofs of (1) and (3) to illustrate

1. \[ (\forall x (P(x) \to Q(x))) \land (\forall x (Q(x) \to R(x))) \]
   Assume
2. \[ (\forall x (P(x) \to Q(x))) \]
   1, taut., MP
3. \[ (\forall x (Q(x) \to R(x))) \]
   1, taut., MP
4. \[ P(x) \to Q(x) \]
   2, AE, MP
5. \[ Q(x) \to R(x) \]
   3, AE, MP
6. \[ P(x) \]
   Assume (towards proving \(P \to R\))
7. \[ Q(x) \]
   4,6, MP
8. \[ R(x) \]
   5,7, MP
9. \[ P(x) \to R(x) \]
   6-8, \(\to\)-introd.
10. \[ \forall x (P(x) \to R(x)) \]
11. \[ \exists x Q(x) \]
   9, AI, x is fresh?
12. we are done by 1-10 \(\to\)-introd.

now for 3. \[ (\forall x P(x)) \land \exists x (P(x) \to Q(x)) \to \exists x Q(x) \]

1. \[ \forall x P(x) \land \exists x (P(x) \to Q(x)) \]
   Assume
2. \[ \forall x P(x) \]
   1, taut., MP
3. \[ \exists x (P(x) \to Q(x)) \]
   1, taut., MP

strategy, take “witness” for 3, apply 2. make deductions, use (EE)
4. \[ P(x) \to Q(x) \]
   Assume
5. \[ P(x) \]
   2, (AE), MP
6. \[ Q(x) \]
   4,5, MP
7. \[ \exists x Q(x) \]
   6, (EI), MP
8. \[ (P(x) \to Q(x)) \to (\exists x Q(x)) \]
   4-8, \(\to\)-introd.
9. \[ (\exists x (P(x) \to Q(x))) \to (\exists x Q(x)) \]
   8, (EE) because x is fresh?
10. \[ \exists x Q(x) \]
   3, 9, MP
11. \[ (\forall x P(x)) \land \exists x (P(x) \to Q(x)) \to \exists x Q(x) \]
   1,10, \(\to\)-introd.

A couple more examples from the book.
P50, section 1.6, 1(c): asks to show that there does not exist integers \( m, n \) so that \( 2m + 4n = 7 \). Their proof is\( \textbf{Suppose} \ m, n \ \textbf{are such integers}. \) then \( 2| (2m) \) and \( 2| (4n) \), hence \( 2| (2m + 4n) \), but \( 2 \nmid 7 \), so this is impossible.

Okay, let’s see. the question is a not there exists statement. Always good idea to try proof by contradiction in these cases. I.e. assume \( \exists \) such \( m, n \). Then their next step is to suppose \( m, n \) have that property (i.e. starting an (EE) style proof). make some integer arithmetic deductions about \( m, n \) and achieve “this is impossible”. Rather we achieve \( 2|7 \) by Leibniz, and \( 2 \nmid 7 \) by “Axiom” and so we have a \( Q \land \neg Q \) situation and have completed a proof by contradiction.

I’ll write out a different version below, then I’ll also do (d) which asks us to show there are no \( m, n \) so that \( 12m + 15n = 1 \). Finally I’ll show that we can change the dummy variable in a quantified expression.

to show there are no integers \( m, n \) so that \( 2m + 4n = 7 \):  
1. \( 2m + 4n = 7 \) Assume (towards a contradiction)  
2. \( 2(m + 2n) = 7 \) 1, Arith., Leibniz  
3. \( \exists k \, 2k = 7 \) 2, (EI), Leibniz  
4. \( 7 \) is even 3, definition, Leibniz  
5. \( 7 \) is odd Arith Axiom  
6. \( 7 \) is not even 5, Arith Axiom  
7. \( (7 \) is even) \land \neg(7 \) is even) 4,7, \land-introd.  
8. \((2m + 4n = 7) \rightarrow (7 \) is even) \land \neg(7 \) is even) 1-7, \rightarrow-introd.

let’s use \( Q \) to stand for “7 is even”  
9. \((\exists n \ (2m + 4n = 7)) \rightarrow (Q \land \neg Q) \) 8, (EE), \( n \) is fresh  
10. \((\exists m \exists n \ (2m + 4n = 7)) \rightarrow (Q \land \neg Q) \) 9, (EE), \( m \) is fresh.  
11. \(\neg(\exists m \exists n \ (2m + 4n = 7)) \) 10, ??? what reasons?

Let me be very careless on (d): assume \( 12m + 15n = 1 \), get \( 3(4m + 5n) = 1 \), get that \( (\exists k) (3k = 1) \), axiom of integers is \( \sim(\exists k) (3k = 1) \). have proven \( (12m + 15n = 1) \) implies \( Q \land \neg Q \) where \( Q \) is the statement that \( 1 \) is a multiple of \( 3 \). By (EE), we have proven that \( (\exists n \ (12m + 15n = 1)) \) implies \( Q \land \neg Q \), and yet again by (EE), we have \( (\exists m \exists n \ (12m + 15n = 1)) \) implies \( Q \land \neg Q \). Since we have a statement implying a contradiction, that statement must be false, hence we have proven its negation. More precisely repeat how you justified line 11 above.
A Hint for 1(e): since you are to prove an $\exists P \rightarrow ??$ statement, set it up like this:

1. $P$ Assume
2. some steps

.. 5. $Q$ somehow 6. $(\exists xQ)$ 5, (EI), MP
7. $P \rightarrow (\exists xQ)$ 1-6, $→$-introd.
8. $(\exists xP) \rightarrow (\exists xQ)$ 7, (EE), $x$ is fresh.

It is useful (even essential) to know that $(\forall xP(x)) \equiv (\forall yP[x;y])$ so long as $x, y$ are fresh. Similarly $(\exists xP(x)) \equiv (\forall yP[x;y])$.

Here’s a proof of $\forall xP(x) \rightarrow \forall yP[x;y]$

1. $\forall x \ x$ is red Assume
2. $y$ is red 1, (AE), MP (check this!)
3. $\forall y \ y$ is red 2, (AI) because no assumptions on $y$.

To prove $(\exists xP) \rightarrow (\exists y P[x;y])$, which obviously has the form $\exists xP \rightarrow ??$ form proceed as follows. I will use $\forall z(3z > x)$ as an example for $P(x)$. Hence $P[x;y]$ will be $\forall z(3z > y)$.

1. $\forall z(3z > x)$ Assume
2. $\exists y \ (\forall z \ (3z > y))$ 1, (EI)
3. $\forall z(3z > x) \rightarrow \exists y \ (\forall z \ (3z > y))$ 1-2, $→$-introd.
4. $(\exists x(\forall z(3z > x))) \rightarrow \exists y \ (\forall z \ (3z > y))$ 3, (EE), $x$ is fresh.