MODUS PONENS (a.k.a. Rule $\longrightarrow$-out)

$$\begin{array}{r} P \longrightarrow Q \\ P \\ \hline Q \end{array}$$

THE CONDITIONAL PROOF RULE (a.k.a. Rule $\longrightarrow$-in)

Rule $\longrightarrow$-in says that **if, assuming P, you prove Q, then you can go to $P \longrightarrow Q$.**
In other words,

$$\begin{array}{ll} & \text{Assume } P \\ & \quad\vdots \\ & Q \\ \hline P \longrightarrow Q & \end{array}$$

(The change in indentation is explained below.)

COMMENT. To apply Rule $\longrightarrow$-in, we proceed as follows: suppose p and q are propositions, and we want to prove $p \longrightarrow q$; we start a "subproof" (i.e., a "proof within a proof", see below) by saying "assume p", and we proceed to proving q. Then we exit the subproof and assert $p \longrightarrow q$ in our main proof.

Notice that to apply this rule **we can introduce any assumptions we want**. It does not matter at all whether the assumptions we introduce are true or false. On the other hand, any time we introduce an assumption p, and we prove something—say a proposition q—using that assumption, then we will not have *proved q*. We will only have *proved q under the assumption p*. Rule $\longrightarrow$-out tells us that, if we do that, then we can "get out from working under the assumption p" and assert the implication $p \longrightarrow q$. But *this does not tell us that q is true*. If we want to conclude that q is true, we need to prove p. (If we can do that, then we can use the Modus Ponens rule to conclude q from p and $p \longrightarrow q$.)

EXAMPLE. If you want to understand how Hamlet must have felt, you could try to imagine that you are Hamlet. That is, you would place yourself under the assumption that you are Hamlet (e.g. by saying to yourself "suppose I was Hamlet") and follow your thoughts. Under that assumption, you might reach the conclusion that you hate your uncle very much and want to punish him for having killed your father and taking his place as king. All these facts (that your uncle killed your father, that you hate him, that you want to punish him) are not true facts in the real world, but are true *in the imaginary world that you entered when you made the assumption that you were Hamlet.* If you want to, you can come out of that imaginary world and, in the real world, draw the conclusion that "if I was Hamlet I would hate my uncle." Your argument would have the following form:

$$\begin{array}{l} \text{Assume I am Hamlet} \\ \qquad \vdots \\ \textit{think, think, think} \\ \qquad \vdots \\ \text{I hate my uncle.} \end{array}$$

If I was Hamlet I would hate my uncle.

This is of the form described in the previous box:

$$\begin{array}{l} \text{Assume } P \\ \vdots \\ Q \end{array}$$

$$P \longrightarrow Q$$

Rule $\wedge$-in

$$\frac{\begin{array}{r} P \\ Q \end{array}}{P \wedge Q}$$

Rule $\wedge$-out

Rule $\wedge$-out is actually a pair of rules, namely, the propositional inference forms

$$\frac{P \wedge Q}{P} \qquad \text{(called"Rule } \wedge\text{-out-a")}$$

and

$$\frac{P \wedge Q}{Q} \qquad \text{(called"Rule } \wedge\text{-out-b")}$$

Rule $\vee$-in

Rule $\vee$-in is actually a pair of rules, namely, the propositional inference forms

$$\frac{(\neg P) \longrightarrow Q}{P \vee Q} \qquad \text{(called "Rule } \vee\text{-in-a")}$$

and

$$\frac{(\neg Q) \longrightarrow P}{P \vee Q} \qquad \text{(called "Rule } \vee\text{-in-b")}$$

COMMENT. Rule $\vee$-in captures the common sense principle that "if you want to show that one of two things is true, it suffices to suppose that one of them is not true and prove the other one." For example:

a. To prove that today must be Monday or Thursday, we prove that if today isn't Monday then it has to be Thursday.

b. To tell your travel agent that you want an aisle seat or a window seat, you could say "if you cannot get me a window seat get me an aisle seat."

COMMENT. In view of Rule $\longrightarrow$-in, to apply Rule $\vee$-in we can use the following format:

$$\begin{array}{ll} & \text{Assume } \neg P \\ & \quad \vdots \\ & Q \\ P \vee Q & \end{array}$$

COMMENT. As special cases of Rule $\vee$-in, we have the following valid propositional inference rules:

$$\frac{P}{P \vee Q}$$

and

$$\frac{Q}{P \vee Q}$$

PROOF BY CASES (a.k.a Rule $\vee$-out)

$$\frac{\begin{array}{c} P \vee Q \\ P \longrightarrow R \\ Q \longrightarrow R \end{array}}{R}$$

PROOF BY CONTRADICTION (a.k.a. Rule ¬-in-out)

$$\begin{array}{r} P \longrightarrow Q \\ \neg Q \\ \hline \neg P \end{array}$$

COMMENT. We labeled Rule ¬-in-out both an "in" rule and an "out" rule because one can think of this rule as a way to *use* a negation (if you have $\neg Q$ you can use this, in conjunction with $P \longrightarrow Q$, to prove something) or as a way to *prove* a negation (since it gives us a way to prove $\neg P$.

COMMENT. A very common use of Rule ¬-in-out is to do **proofs by contradiction**. Suppose you want to prove that something (say a proposition p) is not true. Then you prove that this proposition implies something impossible, i.e., that "if p then q", where q is something that you can prove is not true. This shows that p cannot be true. Using Rule $\longrightarrow$-in (see below) we can carry out our proof y contradiction according to the following format:

$$\begin{array}{l} \vdots \\ \neg q \\ \quad \text{Assume } p \\ \qquad \vdots \\ \quad q \\ p \longrightarrow q \\ \neg p \end{array}$$

or

$$\begin{array}{l} \quad \text{Assume } p \\ \qquad \vdots \\ \quad q \\ p \longrightarrow q \\ \\ \vdots \\ \neg q \\ \neg p \end{array}$$

That is, we make sure that q is impossible, by proving $\neg q$, and then we say "assume p" and go on to prove q; we then conclude the argument by saying "but q is not true, so we have reached a contradiction, and this establishes that p is false."

EXAMPLES OF PROOFS BY CONTRADICTION:

THEOREM: *The number* 30 *cannot be expressed as the difference of the squares of two integers.*

PROOF: Suppose 30 can be expressed as the difference of the squares of two integers. (*Comment: this is a typical proof by contradiction. We want to prove Sthat something isn't true. To do so, we imagine it is true, that is, we explore what things would be like in an imaginary world where it is true. We then set out to show that this imaginary world is impossible, because in it something impossible would have to be true.*) Pick two integers n and m such that $n^2-m^2 = 30$. Then $(n-m)(n+m) = 30$. Now $n+m = (n-m)+2m$. Therefore $n-m$ and $n+m$ are either both odd or both even. If $n-m$ and $n+m$ are both odd then their product, i.e., the number 30, would have to be odd. If $n-m$ and $n+m$ are both even then their product, i.e., the number 30, would have to be divisible by 4. So 30 is either odd or divisible by 4. But this is false, because 30 is neither odd nor divisible by 4. So the assumption that 30 can be expressed as the difference of the squares of two integers leads to an impossible conclusion. Therefore 30 cannot be expressed as the difference of the squares of two integers. $\diamondsuit$

THEOREM: *The number 2 is not the square of a rational number.* (That is, "$\sqrt{2}$ is irrational.")

PROOF: Suppose 2 is the square of a rational number. This means that 2 can be expressed as the quotient of the square of an integer divided by the square of a nonzero integer. Pick two integers n and m such that $2 = \frac{n^2}{m^2}$ and $m \neq 0$. Then, after cancelling all common factors > 1, we may assume that n and m have no common factors > 1. In particular, n and m are not both even, for if they were both even then they would have the factor 2 in common. Now, the equality $2 = \frac{n^2}{m^2}$ implies $2m^2 = n^2$. So n^2 is even. But then n is even, because if n was odd then n^2 would be odd. So $n = 2k$ for some integer k. But then $2m^2 = n^2 = (2k)^2 = 4k^2$. So $m^2 = 2k^2$. So m^2 is even. Then m is even, because if m was odd then m^2 would be odd. Therefore n and m are both even, and at the same time n and m are not both even. These two assertions together add up to an impossible conclusion. Therefore 2 is not the square of a rational number. $\diamondsuit$

Rule $\longleftrightarrow$-in

$$\begin{array}{c} P \longrightarrow Q \\ Q \longrightarrow P \\ \hline P \longleftrightarrow Q \end{array}$$

COMMENT. Often, one uses Rule $\longleftrightarrow$-in as follows. Suppose we want to prove $p \longleftrightarrow q$. Then we prove q assuming p, and p assuming q. For this, we use the following format:

$$
\begin{array}{l}
\vdots \\
\quad \text{Assume } p \\
\quad\quad \vdots \\
\quad q \\
p \longrightarrow q \\
\quad \text{Assume } q \\
\quad\quad \vdots \\
\quad p \\
q \longrightarrow p \\
p \longleftrightarrow q
\end{array}
$$

Rule $\longleftrightarrow$-out

Rule $\longleftrightarrow$-out is actually a pair of rules, namely, the propositional inference forms

$$
\begin{array}{r}
P \longleftrightarrow Q \\
P \\
\hline
Q
\end{array}
\qquad \text{(called“Rule } \longleftrightarrow\text{-out-a”)}
$$

and

$$
\begin{array}{r}
Q \longleftrightarrow P \\
Q \\
\hline
P
\end{array}
\qquad \text{(called“Rule } \longleftrightarrow\text{-out-a”)}
$$

THE TAUTOLOGY PROOF RULE(S)

This “rule” really consists of lots of propositional inference rules, one for each tautology. What these rules say is that if T is a tautology, then

$$
\begin{array}{r}
\hline
T
\end{array}
$$

is a valid propositional inference form.

COMMENT: Notice that in this rule there are no premisses. So what the rule really amounts to is that **you can bring in an instance of a tautology at any point in your proof.**

PROOFS WITHIN PROOFS.

> *Whenever you want, you can start a "subproof," or "proof within a proof," in which you can make* **any assumption you want**. *However, when you do that then all the things you prove are proved* **under that assumption**.

For example, suppose we are reading a mystery novel, and I am trying to prove to you that it was Bob that murdered Bill. Suppose we got to a point where I have established that the murderer must have been Bob or John. Now I want to convince you that it's not John, so it must have been Bob.

Here is one thing I could say: "Suppose John murdered Bill. We know that Bill's body was found in his house, so the killing must have taken place in the house itself, or nearby, because even if the body had been moved it still couldn't have been moved very far. So John must have been in or near Bill's house at the time of the murder. But Bill was killed on September 8 between 9 and 10 p.m. EST. So John must have been in or near Bill's house on September 8 between 9 and 10 p.m. EST. On the other hand, we know that John gave a public lecture in San Diego on September 8, starting at 6 p.m. Pacific time, i.e. at 9 p.m. EST. So he must have traveled from New York to San Diego in one hour or less, which is impossible. So John did not murder Bill."

Notice that what we did here is construct, within our main proof that Bob is the murderer, a "subproof," or "proof within a proof," whose goal is to prove that John is not the murderer. We did this by *introducing a new hypothesis*, namely, by assuming that John is the murderer. In other words, *we created and set out to explore an imaginary world*, in which John did indeed kill Bill, in order to find out what are the consequences and ramifications of the new hypothesis. In this imaginary world, we proved a number of things, such as, for example, that "John traveled from New York to San Diego in one hour or less." But we proved these things *under the hypothesis that John killed Bill.* In order words, we did not really prove that "John traveled from New York to San Diego in one hour or less," but only that this must have been so *if John killed Bill.*

The ultimate consequence of our "proof within a proof" is that this world we have imagined, in which John killed Bill, is impossible, because in this world something impossible happened. So we get out of this "proof within a proof" the conclusion that *John did not kill Bill.* And *this conclusion no longer depends on the new hypothesis that "John killed Bill."* The final conclusion, that *John did not kill Bill*, is valid *without any extra hypotheses*, so it is part of our main proof.

In our mathematical formalism, we are allowed to start a "proof within a proof" any time we want, by assuming anything we want. However, anything we prove will only be part of this "proof within a proof." There will be rules telling us how to get out of the "proof within a proof" and go back to the main proof. The most important one is the following:

RULE $\longrightarrow$-in. (The "conditional proof rule," also called "Rule $\longrightarrow$-in," or "rule for proving an implication.") *If assuming p you get to q then you can go, without assuming p, to $p \longrightarrow q$.*

For example, suppose that the action takes place some time before the November 2000 presidential election. Suppose that, in some argument you are writing, you have established that

(3591) If Gore wins Florida then Gore will become president. (...........)

and, later, that

(4507) If Gore becomes president then the next Attorney General will not be a conservative. (.....................)

That means that, if we use the letters $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ to represent the sentences "Gore wins Florida," "Gore becomes president," and "the next Attorney General will not be a conservative," then we already got

(3591) $\mathcal{A} \longrightarrow \mathcal{B}$. (.....................)
(4507) $\mathcal{B} \longrightarrow \mathcal{C}$. (.....................)

Suppose you just finished writing Step 6812, and now you want to prove $\mathcal{A} \longrightarrow \mathcal{C}$. Here is one thing you could do:

(6813)		Assume $\mathcal{A}$.	(Preparation to apply Rule $\longrightarrow$-in)
(6814)		$\mathcal{B}$.	(Modus Ponens from (3591) and (6813))
(6815)		$\mathcal{C}$.	(Modus Ponens from (4507) and (6814))
(6816)	$\mathcal{A} \longrightarrow \mathcal{C}$.		(Rule $\longrightarrow$-in, from (6813) and (6815))

Steps 6813, 6814, 6815 constitute a "proof within a proof," in which you introduce the new assumption $\mathcal{A}$, and under this assumption you prove first $\mathcal{B}$ and then $\mathcal{C}$. Then in Step 6816 you go back to the main proof, using Rule 4.P.

Notice that we have used extra indentation to indicate that we are writing a proof within a proof. The way we have organized our proof makes it clear that *at no point are we proving $\mathcal{B}$ or $\mathcal{C}$*. We are proving $\mathcal{B}$ and $\mathcal{C}$ *under the assumption* $\mathcal{A}$, from which we can conclude that $\mathcal{A} \longrightarrow \mathcal{C}$, as we do in Step 6816. For all we know, *$\mathcal{B}$ and $\mathcal{C}$ could perfectly well be false*, and nothing in what we wrote says otherwise. (Actually, $\mathcal{B}$ and $\mathcal{C}$ *are* false.) All our "proof within a proof" says is that *if you assume that $\mathcal{A}$ is true, then $\mathcal{C}$ must be true.*

The "proof within a proof" tells us nothing about what happens if $\mathcal{A}$ is false. And our final conclusion, that $\mathcal{A} \to \mathcal{C}$, is of course valid if $\mathcal{A}$ is false, because **an implication such as $\mathcal{A} \to \mathcal{C}$ is true when $\mathcal{A}$ is false.**

INTRODUCING ASSUMPTIONS. Let us look at what we have just said from a slightly different angle.

BOX NO. 1: HYPOTHESES (A.K.A. ASSUMPTIONS).

Hypotheses, or **assumptions**, are statements that we **assume** to be true in a particular situation.
When we discuss proofs later on, we will see that that there are certain statements that you are free to bring in any time you want, because you know them to be true. (Such statements are called "axioms," or "postulates.") In additions, *definitions* function exactly like axioms, the only difference being that an axiom is something you *accept* as true (say, because you are convinced it is true but you do not know how to prove it) whereas a definition (say, for example, $2 = 1 + 1$) is something that you *declare*, or *decide* to be true. **Within a particular proof, hypotheses/assumptions function exactly like axioms and definitions: they are statements that you can bring in any time.** There is, however, a big difference. Axioms and definitions are things that we take to be true forever, because we believe they are true. Hypotheses/assumptions are taken to be true not because we believe they are true, but **because we want to know the consequences of their being true.**
For example: suppose we want to find out what the world would be like if pigs had wings. To do this, we first make the assumption "pigs have wings," by saying

(...) Assume that pigs have wings.

Then we would set out to explore the consequences of this assumption. That is, if you prefer, we would set out to study an **imaginary world** in which pigs have wings, and try to understand what that world would have to be like. We might then be able to "prove" all kind of "theorems," such as

THEOREM 1: *Pigs can fly.*

THEOREM 2: *If a pigsty does not have a roof, then the pigs will fly away.*

(Proving these theorems might not be easy. For example, it is not true that "every animal that has wings can fly," since, for example, ostriches, penguins and dodos do not fly. But you might notice that all the exceptions to the general rule seem to be birds, so perhaps you could make a convincing case that "every animal that has wings and is not a bird can fly." If you manage to do that, then you might go on to argue that pigs can fly, since pigs clearly are not birds.)
All these theorems would be proved **under the hypothesis** that pigs have wings. That is, we would never be saying that we have proved that pigs can fly. All we would be saying is that **IF** pigs had wings **THEN** pigs could fly. In other words, all the facts we would "prove" about pigs under the "pigs have wings" hypothesis would be valid **in the imaginary world of pigs with wings**, which, in principle, is not our real world.

BOX NO. 2: ENTERING AND LEAVING IMAGINARY WORLDS.

As we explained in Box 1, when you assume something you are setting out to explore an **imaginary world**, namely, a world in which that thing you are assuming is true. When can you leave that world and go back to the real world, taking with you the things you have discovered in your imaginary world? The answer is simple: if the thing you assumed is actually true in the real world, then everything you proved **under that assumption** is true, because in that case the imaginary world really is the real world.
Our rules of inference capture this very obvious idea as follows:

- You are always allowed to introduce anything you want as an assumption, any time you want.
- When you do that, whatever you have proved will have been proved **under your assumption**.
- If, assuming a statement $\mathcal{A}$, you prove some other statement $\mathcal{B}$, then you will be allowed to go back to "the real world" and assert there that $\mathcal{A} \longrightarrow \mathcal{B}$.
- If, in addition, you can prove $\mathcal{A}$, then the Modus Ponens rule allows you to go to $\mathcal{B}$.

In simpler terms: whatever you prove under the assumption $\mathcal{A}$ will be valid unrestrictedly (that is, without having to assume that you are under the assumption $\mathcal{A}$) if you can also prove $\mathcal{A}$.

EXAMPLE: If you prove that "pigs can fly" under the assumption that "pigs have wings," then the conclusion that "pigs have wings" will have been established in a world where pigs have wings. You can also go back from such an imaginary world to the real world by stating that "if pigs have wings then pigs can fly." This, however, is not enough to be able to conclude that in the real world pigs can fly, because in the real world you do not know that pigs have wings, and **if you do not know that pigs have wings then you cannot go from "if pigs have wings then pigs can fly" to "pigs can fly."**

HOW COME WE ASSUME THINGS THAT AREN'T KNOWN TO BE TRUE?

A question students frequently ask is:

> **How can I assume something if I don't know that it is is true?**

The answer is very simple:

> **you assume something that you don't know to be true because you want to find out what would happen if it was true. And often *you assume it precisely in order to prove it is not true.***

Often, you prove that something is not true by assuming it is true and exploring the consequences of this assumption until you get to something impossible. This is called "proof by contradiction." We have just seen an example: to prove by contradiction that 30 cannot be expressed as the difference of the squares of two integers, we assumed that 30 could be expressed as the difference of the squares of two integers, and ended up with something false, namely, that 30 is either odd or divisible by 4. That is, **we set out to explore an imaginary world in which** 30 **can be expressed as the difference of the squares of two integers, until we saw that in this world impossible things would haver to happen, and then we concluded that such a world could not exist, so** 30 **cannot be expressed as the difference of the squares of two integers.**

The following four rules are the "in" and "out" rules for each of the two quantifiers. They deal with the following situation:

S1. x is a variable and $\mathcal{A}(x)$ is a formula where there is no x-quantifier,

S2. a is a constant and $\mathcal{A}(a)$ is what you get from $\mathcal{A}(x)$ by substituting a for x in **all** the occurrences of x in $\mathcal{A}(x)$.

EXAMPLE: $\mathcal{A}(x)$ could be the formula $x > a \longrightarrow (\neg\, x = a)$, in which case $\mathcal{A}(a)$ would be the formula $a > a \longrightarrow (\neg\, a = a)$. $\diamondsuit$

THE SPECIALIZATION RULE
(a.k.a. Rule $\forall$-out)

Suppose S1, S2 are true. Then,

$$\frac{\forall x, \mathcal{A}(x)}{\mathcal{A}(a)}\,.$$

EXAMPLE: Suppose $\mathcal{A}(x)$ is the formula $x > a \longrightarrow (\neg\, x = a)$. Then, as explained before, $\mathcal{A}(a)$ is the formula $a > a \longrightarrow (\neg\, a = a)$.

If, in a proof, you got to $\forall x, (x > a \longrightarrow (\neg\, x = a))$, then Rule $\forall$-out enables you to conclude that $a > a \longrightarrow (\neg\, a = a)$.

THE UNIVERSAL GENERALIZATION RULE
(a.k.a. Rule $\forall$-in)

Suppose that S1 and S2 are true. Suppose you are in a proof P (which may be itself be a subproof of some other proof) and you have started a subproof P' of P by saying "Let a be arbitrary," and that until that point a had never appeared in P. Suppose that in P' you got to $\mathcal{A}(a)$. Suppose that $\mathcal{A}(x)$ does not contain a. Then you can get out of P' and go to $\forall x, \mathcal{A}(x)$ in the proof P.

EXAMPLE: Suppose $\mathcal{A}(x)$ is the formula $x \in A \longrightarrow x \in B$, and $\mathcal{B}(x)$ is the formula $x \in B \longrightarrow x \in C$, where A, B, C are constants that stand for sets, and we have, as previous steps in our proof (say in steps 231 and 486), the statements "$A \subseteq B$" and "$B \subseteq C$". Then we can prove $A \subseteq C$ as follows (starting, say, at step 895):

	$\vdots$	
(231)	$A \subseteq B$	
	$\vdots$	
(486)	$B \subseteq C$	
	$\vdots$	
(895)	Let a be arbitrary.	
(896)	$A \subseteq B \longleftrightarrow \forall x, (x \in A \longrightarrow x \in B)$	(Definition of $\subseteq$)
(897)	$\forall x, (x \in A \longrightarrow x \in B)$	(From (231) and (896) by $\longleftrightarrow$-out)
(898)	$B \subseteq C \longleftrightarrow \forall x, (x \in B \longrightarrow x \in C)$	(Definition of $\subseteq$)
(899)	$\forall x, (x \in B \longrightarrow x \in C)$	(From (486) and (898) by $\longleftrightarrow$-out)
(900)	$a \in A \longrightarrow a \in B$	(From (897) by $\forall$-out)
(901)	$a \in B \longrightarrow a \in C$	(From (899) by $\forall$-out)
(902)	Assume $a \in A$.	
(903)	$a \in B$	(From (900) and (902) by $\longrightarrow$-out)
(904)	$a \in C$	(From (903) and (901) by $\longrightarrow$-out)
(905)	$a \in A \longrightarrow a \in C$	(From (902) and (904) by $\longrightarrow$-in)
(906)	$\forall x, (x \in A \longrightarrow x \in C)$	(From (895) and (905) by $\forall$-in)
(907)	$A \subseteq C \longleftrightarrow \forall x, (x \in A \longrightarrow x \in C)$	(Definition of $\subseteq$)
(908)	$A \subseteq C$	(From (906) and (907) by $\longleftrightarrow$-out)

REMARK. You could make the above proof one step shorter by making a clever use of the tautology rule:

$$\vdots$$

(231) $A \subseteq B$

$$\vdots$$

(486) $B \subseteq C$

$$\vdots$$

(895) Let a be arbitrary.

(896) $A \subseteq B \longleftrightarrow \forall x, (x \in A \longrightarrow x \in B)$ (Definition of $\subseteq$)

(897) $\forall x, (x \in A \longrightarrow x \in B)$ (From (231) and (896) by $\longleftrightarrow$-out)

(898) $B \subseteq C \longleftrightarrow \forall x, (x \in B \longrightarrow x \in C)$ (Definition of $\subseteq$)

(899) $\forall x, (x \in B \longrightarrow x \in C)$ (From (486) and (898) by $\longleftrightarrow$-out)

(900) $a \in A \longrightarrow a \in B$ (From (897) by $\forall$-out)

(901) $a \in B \longrightarrow a \in C$ (From (899) by $\forall$-out)

(902) $(a \in A \to a \in B) \to ((a \in B \to a \in C) \to (a \in A \to a \in C))$
(Instance of the tautology $(P \to Q) \to ((Q \to R) \to (P \to R))$)

(903) $(a \in B \to a \in C) \to (a \in A \to a \in C)$
(From (900) and (902) by $\longrightarrow$-out)

(904) $a \in A \longrightarrow a \in C$ (From (901) and (903) by $\longrightarrow$-out)

(905) $\forall x, (x \in A \longrightarrow x \in C)$ (From (895) and (904) by $\forall$-in)

(906) $A \subseteq C \longleftrightarrow \forall x, (x \in A \longrightarrow x \in C)$ (Definition of $\subseteq$)

(907) $A \subseteq C$ (From (905) and (906) by $\longleftrightarrow$-out)

THE EXISTENTIAL GENERALIZATION RULE
(a.k.a. "the witness rule," or "Rule $\exists$-in")

Suppose S1, S2 are true. Suppose you got $\mathcal{A}(a)$ in a previous step. Then you can go to $\exists x, \mathcal{A}(x)$.

COMMENT: This rule says that to prove that "there exists x such that something about x is true" what you can do is exhibit an object a for which the thing is true. Such an a is called a *witness* for $\mathcal{A}(x)$. So, to prove that $\exists x, \mathcal{A}(x)$, you find a witness.

EXAMPLE. *Prove that* $\exists x, (x \in \mathbb{Z} \wedge x + 5 = 12)$.

PROOF.
$7 \in \mathbb{Z} \wedge 7 + 5 = 12$
$\exists x, (x \in \mathbb{Z} \wedge x + 5 = 12)$

THE EXISTENTIAL SPECIALIZATION RULE
(a.k.a. "Rule ∃-out")

Suppose S1, S2 are true. Suppose you have $\exists x, \mathcal{A}(x)$ in a proof P (which could itself be a subproof of another proof). Then you can start a sub-subproof P' within P by saying "Pick a such that $\mathcal{A}(a)$," provided that until that point a had never appeared in P. Suppose that in P' you get $\mathcal{B}$, where $\mathcal{B}$ is a sentence that does not contain the constant a. Then you can get out of P' and go to $\mathcal{B}$ in P.
In other words:

$$\begin{array}{ll} \exists x, \mathcal{A}(x) & \\ & \text{Pick } a \text{ such that } \mathcal{A}(a) \\ & \vdots \\ & \mathcal{B} \\ \hline \mathcal{B} & \end{array}$$

provided that a has not appeared before the "PIck a" step, and $\mathcal{B}$ does not contain a.

EXAMPLE. Suppose m, n are integers, $n|m$, $n > 0$, $m > 0$, and n is composite. Prove that m is composite.

PROOF. Since n is composite, $n > 1$ and $\exists x, (x|n \wedge 1 < x \wedge x < n)$. Pick one such x and call it a. Then $a > 1$, $a < n$, and $a|n$. Since $a|n$, $\exists x, n = a.x$. Pick one such x and call it b. Then $n = a.b$. Since $n|m$, $\exists x, m = n.x$. Pick one such x and call it c. Then $m = n.c$. So $m = (a.b).c = a.(b.c)$. Therefore $\exists x, m = a.x$. So $a|m$. Furthermore, $n \leq m$, because $n > 0$, $m > 0$, and $n|m$. Since $a < n$, it follows that $a < m$. So $a > 1 \wedge a < m \wedge a|m$. Therefore $\exists x, (x > 1 \wedge x < m \wedge x|m)$. So m is composite. ♢

The following example shows that if you do not apply Rule ∃-out correctly you can "prove" things that are false.

THE PEANO PARADOX

THEOREM: 1 is the largest natural number.

PROOF: Let n be the largest natural number. Then n^2 is a natural number too. Since n was the largest natural number, $n^2 \leq n$. On the other hand, $n \geq 1$, so $n^2 = n.n \geq n.1 = n$. So $n^2 \leq n$ and $n^2 \geq n$. Therefore $n^2 = n$. The only solutions x of $x^2 = x$ are $x = 1$ and $x = 0$. So $n = 1$ or $n = 0$. But 0 is not a natural number, so n cannot be 0. Therefore n has to be equal to 1. **QED**