X4.2 Let P and Q be specifications, let I be an assertion with all nonlocal variables unprimed, and let I' be the same as I but with primes on all nonlocal variables. Prove

(a) $I \Rightarrow I' \,.\, I \Rightarrow I' \implies I \Rightarrow I'$

(b) If I is invariant for P, and I is invariant for Q, then I is invariant for $(P.Q)$.

After trying the question, scroll down to the solution.

(a) $I \Rightarrow I' \,.\, I \Rightarrow I' \;\Longrightarrow\; I \Rightarrow I'$

§

$$
\begin{array}{lll}
 & I \Rightarrow I' \,.\, I \Rightarrow I' & \text{rewrite with explicit arguments} \\
= & I\,\sigma \Rightarrow I\,\sigma' \;.\; I\,\sigma \Rightarrow I\,\sigma' & \text{sequential composition} \\
= & \exists \sigma'' \cdot (I\,\sigma \Rightarrow I\,\sigma'') \wedge (I\,\sigma'' \Rightarrow I\,\sigma') & \text{transitivity} \\
\Longrightarrow & \exists \sigma'' \cdot I\,\sigma \Rightarrow I\,\sigma' & \text{unused quantifier} \\
= & I\,\sigma \Rightarrow I\,\sigma' & \text{rewrite with implicit arguments} \\
= & I \Rightarrow I' &
\end{array}
$$

(b) If I is invariant for P, and I is invariant for Q, then I is invariant for $(P.Q)$.

§ We are given I is invariant for P, which means $(I \Rightarrow I') \Leftarrow P$ is a theorem.
We are given I is invariant for Q, which means $(I \Rightarrow I') \Leftarrow Q$ is a theorem.
We want to prove I is invariant for $(P.Q)$, which means $(I \Rightarrow I') \Leftarrow (P.Q)$ is a theorem.
One of the Refinement by Steps laws says: If $A \Leftarrow B.C$ and $B \Leftarrow D$ and $C \Leftarrow E$ are theorems, then $A \Leftarrow D.E$ is a theorem. Let A, B, and C all be $I \Rightarrow I'$; let D be P; let E be Q. Then we have $(A \Leftarrow B.C)$ by part (a). We have $(B \Leftarrow D)$ because I is invariant for P. And we have $(C \Leftarrow E)$ because I is invariant for Q. So by Refinement by Steps, we have $(A \Leftarrow D.E)$, which says I is invariant for $(P.Q)$.

There must be a nice calculational proof.