Problem 1

Give a formal proof of the valid assertion

\[ \left( (x \mapsto y \ast x' \mapsto y') \ast \text{true} \right) \Rightarrow \]
\[ \left( (x \mapsto y \ast \text{true}) \land (x' \mapsto y' \ast \text{true}) \right) \wedge x \neq x' \]

from the rules on page 120 of Chapter 3 of the class notes, and (some of) the following inference rules for predicate calculus:

\[ p \Rightarrow \text{true} \quad p \Rightarrow p \quad p \land \text{true} \Rightarrow p \]

\[ p \Rightarrow q \quad q \Rightarrow r \quad (\text{trans impl}) \]

\[ p \Rightarrow r \]

\[ p \Rightarrow q \quad p \Rightarrow r \quad (\land\text{-introduction}) \]

\[ p \Rightarrow q \land r \]

Your proof will be easier to read if you write it as a sequence of steps rather than a tree. In the inference rules, you should regard \( \ast \) as left associative, e.g.,

\[ e_1 \mapsto e_1' \ast e_2 \mapsto e_2' \ast \text{true} \Rightarrow e_1 \neq e_2 \]

stands for

\[ (e_1 \mapsto e_1' \ast e_2 \mapsto e_2') \ast \text{true} \Rightarrow e_1 \neq e_2. \]

For brevity, you may weaken \( \iff \) to \( \Rightarrow \) when it is the main operator of an axiom. You may also omit instances of the axiom schema \( p \Rightarrow p \) when it is used as a premiss of the monotonicity rule.
Problem 2

None of the following axiom schemata are sound. For each, given an instance which is not valid, along with a description of a state in which the instance is false.

\[ p_1 \ast p_2 \neq p_1 \land p_2 \]
\[ p_1 \land p_2 \neq p_1 \ast p_2 \]
\[ (p_1 \ast p_2) \lor q \neq (p_1 \lor q) \ast (p_2 \lor q) \]
\[ (p_1 \lor q) \ast (p_2 \lor q) \neq (p_1 \ast p_2) \lor q \]
\[ (p_1 \ast q) \land (p_2 \ast q) \neq (p_1 \land p_2) \ast q \]
\[ (p_1 \ast p_2) \land q \neq (p_1 \land q) \ast (p_2 \land q) \]
\[ (p_1 \land q) \ast (p_2 \land q) \neq (p_1 \ast p_2) \land q \]

\[ (\forall x. (p_1 \ast p_2)) \neq (\forall x. p_1) \ast p_2 \quad \text{when } x \text{ not free in } p_2 \]
\[ (p_1 \Rightarrow p_2) \neq \left( (p_1 \ast q) \Rightarrow (p_2 \ast q) \right) \]
\[ (p_1 \Rightarrow p_2) \neq (p_1 \Rightarrow p_2) \]
\[ (p_1 \Rightarrow p_2) \neq (p_1 \Rightarrow p_2) \]

Problem 3

Fill in the postconditions in

\[ \{ (e_1 \Rightarrow -) \ast (e_2 \Rightarrow -) \} \mid [e_1] := e'_1 ; [e_2] := e'_2 \{ ? \} \]
\[ \{ (e_1 \Rightarrow -) \land (e_2 \Rightarrow -) \} \mid [e_1] := e'_1 ; [e_2] := e'_2 \{ ? \}. \]

to give two sound inference rules describing a sequence of two mutations. Your postconditions should be as strong as possible.

Give a derivation of each of these inference rules, exhibited as an annotated specification.