Homework Assignment #3

Due Time/Date

2:20PM Wednesday, October 16, 2024. Late submission will be penalized by 20% for each working day overdue.

How to Submit

Please email your completed homework in one single .v file to the instructor by the due time. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

All the problems must be solved using Coq. In the problem statements, we assume the binding powers of the logical connectives and the entailment symbol decrease in this order: $\neg$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\vdash$.

1. (30 points) Formalize the following sequents and prove their validity:
   (a) $\vdash (p \rightarrow r) \wedge (q \rightarrow r) \rightarrow p \vee q \rightarrow r$
   (b) $\vdash (p \vee q \rightarrow r) \rightarrow (p \rightarrow r) \wedge (q \rightarrow r)$
2. (30 points) Formalize the following sequents and prove their validity:
   (a) $\forall x(P(x) \rightarrow Q(x)) \vdash \exists x P(x) \rightarrow \exists x Q(x)$
   (b) $\vdash \exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$
3. (40 points) A first-order theory for *groups* contains the following three axioms:
   - $\forall a \forall b \forall c(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$. (Associativity)
   - $\forall a((a \cdot e = a) \wedge (e \cdot a = a))$. (Identity)
   - $\forall a((a \cdot a^{-1} = e) \wedge (a^{-1} \cdot a = e))$. (Inverse)

   Here $\cdot$ is the binary operation, e is a constant, called the identity, and $(\cdot)^{-1}$ is the inverse function which gives the inverse of an element. Let M denote the set of the three axioms subsequently, for brevity. Formalize the following sequent and prove its validity:

   $M \vdash \forall a \forall b \forall c((b \cdot a = c \cdot a) \rightarrow b = c)$,

   which states the right cancellation property.

   (Hint: a typical proof in algebra books is the following: $b = b \cdot e = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = (c \cdot a) \cdot a^{-1} = c \cdot (a \cdot a^{-1}) = c \cdot e = c$.)