Homework Assignment #3

Note

This assignment is due 2:20PM Thursday, November 17, 2011. Please write or type your answers on A4 (or similar size) paper. Put your completed homework on the instructor's desk before the class starts. For late submissions, please drop them in Yih-Kuen Tsay's mail box on the first floor of Management Building II. A late submission will be penalized by 20% for each working day overdue. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

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. 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. Prove, using *Natural Deduction* plus the derived rules in HW#2, the validity of the following sequents:

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

   (20 points)

   (b) $M \vdash \forall a \forall b \forall c (((a \cdot b = e) \wedge (b \cdot a = e) \wedge (a \cdot c = e) \wedge (c \cdot a = e)) \rightarrow b = c)$, which says that every element has a unique inverse. (Hint: a typical proof in algebra books is the following: $b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$.) (20 points)

2. Prove that the following annotated program segments are correct:

   (a) $\{true\}$
   if $x < y$ **then** $x, y := y, x$ **fi**
   $\{x \geq y\}$

   (10 points)

(b) $\{g = 0 \land p = n \land n \geq 1\}$

    while $p \geq 2$ **do**

        $g, p := g + 1, p - 1$

    od

    $\{g = n - 1\}$

(20 points)

(c) For this program, prove its total correctness.

$\{y > 0 \land (x \equiv m \pmod{y})\}$

while $x \geq y$ **do**

    $x := x - y$

od

$\{(x \equiv m \pmod{y}) \land x < y\}$

(30 points)