Suggested Solutions for Homework Assignment #3

We assume the binding powers of the logical connectives and the entailment symbol decrease in this order: $\neg$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\to$, $\leftrightarrow$, $\vdash$.

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\alpha \qquad \delta}{M, x \cdot y = x \cdot z \vdash y = z}\,(=E)}{M \vdash (x \cdot y = x \cdot z) \to y = z}\,(\to I)}{M \vdash \forall c((x \cdot y = x \cdot c) \to y = c)}\,(\forall I)}{M \vdash \forall b \forall c((x \cdot b = x \cdot c) \to b = c)}\,(\forall I)}{M \vdash \forall a \forall b \forall c((a \cdot b = a \cdot c) \to b = c)}\,(\forall I)$$

α :

$$\dfrac{\dfrac{\beta \qquad \gamma}{M, x \cdot y = x \cdot z \vdash (x^{-1} \cdot x) \cdot y = y}\,(=E) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{M, x \cdot y = x \cdot z \vdash \forall a \forall b \forall c (a \cdot (b \cdot c) = (a \cdot b) \cdot c)}\,(Hyp)}{M, x \cdot y = x \cdot z \vdash \forall b \forall c (x^{-1} \cdot (b \cdot c) = (x^{-1} \cdot b) \cdot c)}\,(\forall E)}{M, x \cdot y = x \cdot z \vdash \forall c (x^{-1} \cdot (x \cdot c) = (x^{-1} \cdot x) \cdot c)}\,(\forall E)}{M, x \cdot y = x \cdot z \vdash x^{-1} \cdot (x \cdot y) = (x^{-1} \cdot x) \cdot y}\,(\forall E)}{M, x \cdot y = x \cdot z \vdash x^{-1} \cdot (x \cdot y) = y}\,(=E)$$

β :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{M, x \cdot y = x \cdot z \vdash \forall a (a \cdot a^{-1} = e \wedge a^{-1} \cdot a = e)}\,(Hyp)}{M, x \cdot y = x \cdot z \vdash x \cdot x^{-1} = e \wedge x^{-1} \cdot x = e}\,(\forall E)}{M, x \cdot y = x \cdot z \vdash x^{-1} \cdot x = e}\,(\wedge E_2)}{M, x \cdot y = x \cdot z \vdash e = x^{-1} \cdot x}\,(= Symmetry)$$

γ :

$$\dfrac{\dfrac{\dfrac{}{M, x \cdot y = x \cdot z \vdash \forall a (a \cdot e = a \wedge e \cdot a = a)}\,(Hyp)}{M, x \cdot y = x \cdot z \vdash y \cdot e = y \wedge e \cdot y = y}\,(\forall E)}{M, x \cdot y = x \cdot z \vdash e \cdot y = y}\,(\wedge E_2)$$

δ :

$$\dfrac{\dfrac{\dfrac{}{M, x\cdot y = x\cdot z \vdash x\cdot y = x\cdot z}\,(\mathit{Hyp})}{M, x\cdot y = x\cdot z \vdash x\cdot z = x\cdot y}\,(= \mathit{Symmetry}) \qquad \dfrac{\text{the proof tree is similar to } \alpha}{M, x\cdot y = x\cdot z \vdash x^{-1}\cdot(x\cdot z) = z}}{M, x\cdot y = x\cdot z \vdash x^{-1}\cdot(x\cdot y) = z}\,(= E)$$

□

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

Solution. We use N to denote $x\cdot y = e \wedge y\cdot x = e \wedge x\cdot z = e \wedge z\cdot x = e$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(1)\alpha \qquad (1)\delta}{M, N, x\cdot y = x\cdot z \vdash y = z}\,(= E)}{M, N \vdash x\cdot y = x\cdot z \to y = z}\,(\to I) \qquad \dfrac{\alpha \qquad \beta}{M, N \vdash x\cdot y = x\cdot z}\,(= E)}{M, N \vdash y = z}\,(\to E)}{M \vdash (x\cdot y = e \wedge y\cdot x = e \wedge x\cdot z = e \wedge z\cdot x = e) \to y = z}\,(\to I)}{M \vdash \forall c((x\cdot y = e \wedge y\cdot x = e \wedge x\cdot c = e \wedge c\cdot x = e) \to y = c)}\,(\forall I)}{M \vdash \forall b \forall c((x\cdot b = e \wedge b\cdot x = e \wedge x\cdot c = e \wedge c\cdot x = e) \to b = c)}\,(\forall I)}{M \vdash \forall a \forall b \forall c((a\cdot b = e \wedge b\cdot a = e \wedge a\cdot c = e \wedge c\cdot a = e) \to b = c)}\,(\forall I)$$

α :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{M, N \vdash x\cdot y = e \wedge y\cdot x = e \wedge x\cdot z = e \wedge z\cdot x = e}\,(\mathit{Hyp})}{M, N \vdash x\cdot z = e \wedge z\cdot x = e}\,(\wedge E_2)}{M, N \vdash x\cdot z = e}\,(\wedge E_1)}{M, N \vdash e = x\cdot z}\,(= \mathit{Symmetry})$$

β :

$$\dfrac{\dfrac{}{M, N \vdash x\cdot y = e \wedge y\cdot x = e \wedge x\cdot z = e \wedge z\cdot x = e}\,(\mathit{Hyp})}{M, N \vdash x\cdot y = e}\,(\wedge E_1)$$

□

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

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

Solution.

$$\dfrac{\dfrac{\dfrac{\text{pred. calculus + algebra}}{\mathit{true} \wedge x < y \to y \geq x} \qquad \dfrac{}{\{\ y \geq x\ \}\ x, y := y, x\ \{\ x \geq y\ \}}\,(\text{Assign})}{\{\ \mathit{true} \wedge x < y\ \}\ x, y := y, x\ \{\ x \geq y\ \}}\,(\text{SP}) \qquad \dfrac{\text{pred. calculus + algebra}}{\mathit{true} \wedge \neg(x < y) \to x \geq y}}{\{\ \mathit{true}\ \}\ \textbf{if}\ x < y\ \textbf{then}\ x, y := y, x\ \textbf{fi}\ \{\ x \geq y\ \}}\,(\text{If-Then})$$

□

(b) $\{g = 0 \wedge p = n \wedge n \geq 1\}$
while $p \geq 2$ **do**
$g, p := g + 1, p - 1$
od
$\{g = n - 1\}$
Solution.

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{g = 0 \land p = n \land n = 1 \to p > 0 \land p + g = n} \qquad \alpha \qquad \dfrac{\text{pred. calculus + algebra}}{p > 0 \land p + g = n \land \neg(p \geq 2) \to g = n - 1}}{\{\ g = 0 \land p = n \land n = 1\ \}\ \textbf{while}\ p \geq 2\ \textbf{do}\ g, p := g - 1, p + 1\ \textbf{od}\ \{\ g = n - 1\ \}}\ (\text{Consequence})$$

α :

$$\dfrac{\beta \qquad \dfrac{\dfrac{}{\{\ p + 1 > 0 \land (p + 1) + (g - 1) = n\ \}\ g, p := g - 1, p + 1\ \{\ p > 0 \land p + g = n\ \}}\ (\text{Assign})}{\{\ p > 0 \land p + g = n \land p \geq 2\ \}\ g, p := g - 1, p + 1\ \{\ p > 0 \land p + g = n\ \}}\ (\text{SP})}{\{\ p > 0 \land p + g = n\ \}\ \textbf{while}\ p \geq 2\ \textbf{do}\ g, p := g - 1, p + 1\ \textbf{od}\ \{\ p > 0 \land p + g = n \land \neg(p \geq 2)\ \}}\ (\text{while})$$

β :

$$\dfrac{\text{pred. calculus + algebra}}{p > 0 \land p + g = n \land p \geq 2 \to p + 1 > 0 \land (p + 1) + (g - 1) = n}$$

□

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

Solution.

$$\dfrac{\alpha \qquad \dfrac{\text{pred. calculus + algebra}}{y > 0 \land (x \equiv m \pmod y) \land \neg(x \geq y) \to (x \equiv m \pmod y) \land x < y}}{\{\ y > 0 \land (x \equiv m \pmod y)\ \}\ \textbf{while}\ x \geq y\ \textbf{do}\ x := x - y\ \textbf{od}\ \{\ (x \equiv m \pmod y) \land x < y\ \}}\ (\text{SP})$$

α :

$$\dfrac{\beta \qquad \gamma \qquad \dfrac{\text{pred. calculus + algebra}}{y > 0 \land (x \equiv m \pmod y) \land x \geq y \to x \geq 0}}{\{\ y > 0 \land (x \equiv m \pmod y)\ \}\ \textbf{while}\ x \geq y\ \textbf{do}\ x := x - y\ \textbf{od}\ \{\ y > 0 \land (x \equiv m \pmod y) \land \neg(x \geq y)\ \}}\ (\text{while: simply total})$$

β :

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{y > 0 \land (x \equiv m \pmod y) \land x \geq y \to y > 0 \land ((x - y) \equiv m \pmod y)} \qquad \dfrac{}{\{\ y > 0 \land ((x - y) \equiv m \pmod y)\ \}\ x := x - y\ \{\ y > 0 \land (x \equiv m \pmod y)\ \}}\ (\text{Assign})}{\{\ y > 0 \land (x \equiv m \pmod y) \land x \geq y\ \}\ x := x - y\ \{\ y > 0 \land (x \equiv m \pmod y)\ \}}\ (\text{SP})$$

γ :

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{y > 0 \land (x \equiv m \pmod y) \land x \geq y \land x = Z \to x - y < Z} \qquad \dfrac{}{\{\ x - y < Z\ \}\ x := x - y\ \{\ x < Z\ \}}\ (\text{Assign})}{\{\ y > 0 \land (x \equiv m \pmod y) \land x \geq y \land x = Z\ \}\ x := x - y\ \{\ x < Z\ \}}\ (\text{SP})$$

□