CS486 Problem Set 9 DUE: 4/17/03

1. a) We give a finite model of a semigroup that is not commutative.

$$D = \{\mathsf{a}, \mathsf{b}\}$$

$$== \{(\mathsf{a}, \mathsf{a}), (\mathsf{b}, \mathsf{b})\}$$

$X \circ Y = X$		
$\circ$	a	b
a	a	a
b	b	b

Clearly, $=$ satisfies ref, sym, and trans. Likewise, $\circ$ satisifies subst, functionality, and assoc. Hence, $\langle D, =, \circ \rangle$ is a semigroup. Furthermore, $\mathsf{a} \circ \mathsf{b} = \mathsf{a} \neq \mathsf{b} = \mathsf{b} \circ \mathsf{a}$; hence $\langle D, =, \circ \rangle$ is not a commutative semigroup.

b) We give a finite model of a commutative semigroup that is not a monoid.

$$D = \{\mathsf{a}, \mathsf{b}\}$$

$$== \{(\mathsf{a}, \mathsf{a}), (\mathsf{b}, \mathsf{b})\}$$

$X \circ Y = \mathsf{a}$		
$\circ$	a	b
a	a	a
b	a	a

Clearly, $=$ satisfies ref, sym, and trans. Likewise, $\circ$ satisifies subst, functionality, assoc, and comm. Hence, $\langle D, =, \circ \rangle$ is a commutative semigroup. Furthermore, $\circ$ does not satisfy ident; hence $\langle D, =, \circ \rangle$ is not a monoid.

2. Consider the Boolean ring $\langle \mathbb{B}, =, \Leftrightarrow, \vee, \mathbf{T}, \mathbf{F} \rangle$; that is, in addition to the ring axioms, we assume the following axiom:

$$\texttt{idemp}_{\vee}: \quad (\forall x)(x \vee x = x)$$

We also assume the following axiom (although it may be provable from the previous axioms):

$$\texttt{const}_{\Leftrightarrow}: \quad (\forall x)(x \Leftrightarrow x = \mathbf{T})$$

We first prove two useful derived theorems:

$\texttt{ident}_{\Leftrightarrow}\texttt{-with}_{\vee}$: $(\forall x)((x \vee \mathbf{T} = \mathbf{T}) \wedge (\mathbf{T} \vee x = \mathbf{T}))$

(1)	$\mathbf{T} = (\mathbf{T} \Leftrightarrow \mathbf{T})$	$\texttt{ident}_{\Leftrightarrow}$
(2)	$(x \vee \mathbf{T}) = (x \vee \mathbf{T})$	refl
(3)	$(x \vee \mathbf{T}) = (x \vee (\mathbf{T} \Leftrightarrow \mathbf{T}))$	subst{1,2}
(4)	$(x \vee (\mathbf{T} \Leftrightarrow \mathbf{T})) = ((x \vee \mathbf{T}) \Leftrightarrow (x \vee \mathbf{T}))$	distrib
(5)	$(x \vee \mathbf{T}) = ((x \vee \mathbf{T}) \Leftrightarrow (x \vee \mathbf{T}))$	subst{4,3}
(6)	$((x \vee \mathbf{T}) \Leftrightarrow \overline{(x \vee \mathbf{T})}) = \mathbf{T}$	$\texttt{inv}_{\Leftrightarrow}$
(7)	$(((x \vee \mathbf{T}) \Leftrightarrow (x \vee \mathbf{T})) \Leftrightarrow \overline{(x \vee \mathbf{T})}) = \mathbf{T}$	subst{5,6}
(8)	$(((x \vee \mathbf{T}) \Leftrightarrow (x \vee \mathbf{T})) \Leftrightarrow \overline{(x \vee \mathbf{T})}) = ((x \vee \mathbf{T}) \Leftrightarrow ((x \vee \mathbf{T}) \Leftrightarrow \overline{(x \vee \mathbf{T})}))$	$\texttt{assoc}_{\Leftrightarrow}$
(9)	$((x \vee \mathbf{T}) \Leftrightarrow ((x \vee \mathbf{T}) \Leftrightarrow \overline{(x \vee \mathbf{T})})) = \mathbf{T}$	subst{8,7}
(10)	$((x \vee \mathbf{T}) \Leftrightarrow \mathbf{T}) = \mathbf{T}$	subst{6,9}
(11)	$((x \vee \mathbf{T}) \Leftrightarrow \mathbf{T}) = (x \vee \mathbf{T})$	$\texttt{ident}_{\Leftrightarrow}$
(12)	$(x \vee \mathbf{T}) = \mathbf{T}$	subst{11,10}

(1)	$\mathbf{T} = (\mathbf{T} \Leftrightarrow \mathbf{T})$	$\texttt{ident}_{\Leftrightarrow}$
(2)	$(\mathbf{T} \vee x) = (\mathbf{T} \vee x)$	refl
(3)	$(\mathbf{T} \vee x) = ((\mathbf{T} \Leftrightarrow \mathbf{T}) \vee x)$	subst{1,2}
(4)	$((\mathbf{T} \Leftrightarrow \mathbf{T}) \vee x) = ((\mathbf{T} \vee x) \Leftrightarrow (\mathbf{T} \vee x))$	distrib
(5)	$(\mathbf{T} \vee x) = ((\mathbf{T} \vee x) \Leftrightarrow (\mathbf{T} \vee x))$	subst{4,3}
(6)	$((\mathbf{T} \vee x) \Leftrightarrow \overline{(\mathbf{T} \vee x)}) = \mathbf{T}$	$\texttt{inv}_{\Leftrightarrow}$
(7)	$(((\mathbf{T} \vee x) \Leftrightarrow (\mathbf{T} \vee x)) \Leftrightarrow \overline{(\mathbf{T} \vee x)}) = \mathbf{T}$	subst{5,6}
(8)	$(((\mathbf{T} \vee x) \Leftrightarrow (\mathbf{T} \vee x)) \Leftrightarrow \overline{(\mathbf{T} \vee x)}) = ((\mathbf{T} \vee x) \Leftrightarrow ((\mathbf{T} \vee x) \Leftrightarrow \overline{(\mathbf{T} \vee x)}))$	$\texttt{assoc}_{\Leftrightarrow}$
(9)	$((\mathbf{T} \vee x) \Leftrightarrow ((\mathbf{T} \vee x) \Leftrightarrow \overline{(\mathbf{T} \vee x)})) = \mathbf{T}$	subst{8,7}
(10)	$((\mathbf{T} \vee x) \Leftrightarrow \mathbf{T}) = \mathbf{T}$	subst{6,9}
(11)	$((\mathbf{T} \vee x) \Leftrightarrow \mathbf{T}) = (\mathbf{T} \vee x)$	$\texttt{ident}_{\Leftrightarrow}$
(12)	$(\mathbf{T} \vee x) = \mathbf{T}$	subst{11,10}

$\texttt{comm}_\vee$: $(\forall x, y)(x \vee y = y \vee x)$

(1)	$(x \vee x) = x$	$\texttt{idemp}_\vee$
(2)	$(y \vee y) = y$	$\texttt{idemp}_\vee$
(3)	$((x \Leftrightarrow y) \vee (x \Leftrightarrow y)) = (x \Leftrightarrow y)$	$\texttt{idemp}_\vee$
(4)	$((x \Leftrightarrow y) \vee (x \Leftrightarrow y)) = ((x \vee x) \Leftrightarrow (x \vee y) \Leftrightarrow (y \vee x) \Leftrightarrow (y \vee y))$	distrib
(5)	$((x \Leftrightarrow y) \vee (x \Leftrightarrow y)) = (x \Leftrightarrow (x \vee y) \Leftrightarrow (y \vee x) \Leftrightarrow (y \vee y))$	subst{1,4}
(6)	$((x \Leftrightarrow y) \vee (x \Leftrightarrow y)) = (x \Leftrightarrow (x \vee y) \Leftrightarrow (y \vee x) \Leftrightarrow y)$	subst{2,5}
(7)	$(x \Leftrightarrow y) = (x \Leftrightarrow (x \vee y) \Leftrightarrow (y \vee x) \Leftrightarrow y)$	subst{3,6}
(8)	$(x \Leftrightarrow y) = ((x \vee y) \Leftrightarrow (y \vee x) \Leftrightarrow x \Leftrightarrow y)$	$\texttt{assoc}_\Leftrightarrow$
(9)	$((x \Leftrightarrow y) \Leftrightarrow \overline{(x \Leftrightarrow y)}) = \mathbf{T}$	$\texttt{ident}_\Leftrightarrow$
(10)	$(((x \vee y) \Leftrightarrow (y \vee x) \Leftrightarrow x \Leftrightarrow y) \Leftrightarrow \overline{(x \Leftrightarrow y)}) = \mathbf{T}$	subst{9,8}
(11)	$(((x \vee y) \Leftrightarrow (y \vee x)) \Leftrightarrow ((x \Leftrightarrow y) \Leftrightarrow \overline{(x \Leftrightarrow y)})) = \mathbf{T}$	$\texttt{assoc}_\Leftrightarrow$
(12)	$(((x \vee y) \Leftrightarrow (y \vee x)) \Leftrightarrow \mathbf{T}) = \mathbf{T}$	subst{9,11}
(13)	$((x \vee y) \Leftrightarrow (y \vee x)) = \mathbf{T}$	$\texttt{ident}_\Leftrightarrow$
(14)	$(x \vee \mathbf{T}) = \mathbf{T}$	$\texttt{ident}_\Leftrightarrow\texttt{-with}_\vee$
(15)	$(x \vee ((x \vee y) \Leftrightarrow (y \vee x))) = \mathbf{T}$	subst{13,14}
(16)	$((x \vee x \vee y) \Leftrightarrow (x \vee y \vee x)) = \mathbf{T}$	distrib
(17)	$((x \vee y) \Leftrightarrow (x \vee y \vee x)) = \mathbf{T}$	subst{1,16}
(18)	$(\mathbf{T} \vee x) = \mathbf{T}$	$\texttt{ident}_\Leftrightarrow\texttt{-with}_\vee$
(19)	$(((x \vee y) \Leftrightarrow (y \vee x)) \vee x) = \mathbf{T}$	subst{13,18}
(20)	$((x \vee y \vee x) \Leftrightarrow (y \vee x \vee x)) = \mathbf{T}$	distrib
(21)	$((x \vee y \vee x) \Leftrightarrow (y \vee x)) = \mathbf{T}$	subst{1,20}
(22)	$((y \vee x) \Leftrightarrow (x \vee y \vee x)) = \mathbf{T}$	$\texttt{comm}_\Leftrightarrow$
(23)	$(x \vee y \vee x) \Leftrightarrow \overline{(x \vee y \vee x)} = \mathbf{T}$	$\texttt{ident}_\Leftrightarrow$
(24)	$(\mathbf{T} \Leftrightarrow \overline{(x \vee y \vee x)}) = (\mathbf{T} \Leftrightarrow \overline{(x \vee y \vee x)})$	refl
(25)	$((x \vee y) \Leftrightarrow (x \vee y \vee x) \Leftrightarrow \overline{(x \vee y \vee x)}) = (\mathbf{T} \Leftrightarrow \overline{(x \vee y \vee x)})$	subst{17,24}
(26)	$((x \vee y) \Leftrightarrow (x \vee y \vee x) \Leftrightarrow \overline{(x \vee y \vee x)}) = ((y \vee x) \Leftrightarrow (x \vee y \vee x) \Leftrightarrow \overline{(x \vee y \vee x)})$	subst{22,25}
(27)	$((x \vee y) \Leftrightarrow \mathbf{T}) = ((y \vee x) \Leftrightarrow \mathbf{T})$	subst{23,26}
(28)	$((x \vee y) \Leftrightarrow \mathbf{T}) = (x \vee y)$	$\texttt{ident}_\Leftrightarrow$
(29)	$((y \vee x) \Leftrightarrow \mathbf{T}) = (y \vee x)$	$\texttt{ident}_\Leftrightarrow$
(30)	$(x \vee y) = ((y \vee x) \Leftrightarrow \mathbf{T})$	subst{28,27}
(31)	$(x \vee y) = (y \vee x)$	subst{29,30}

Define $\sim$, $\wedge$, and $\supset$ as follows:

$$\begin{array}{rcl} \sim x & \equiv & x \Leftrightarrow \mathbf{F} \\ x \wedge y & \equiv & (x \vee y) \Leftrightarrow (x \Leftrightarrow y) \\ x \supset y & \equiv & (x \Leftrightarrow \mathbf{F}) \vee y \end{array}$$

We prove the following laws using the Boolean ring axioms:

(1) $p \supset (p \vee q)$

$$\begin{array}{rcll} p \supset (p \vee q) & = & (p \Leftrightarrow \mathbf{F}) \vee (p \vee q) & \supset\texttt{-def} \\ & = & (p \vee (p \vee q)) \Leftrightarrow (\mathbf{F} \vee (p \vee q)) & \texttt{distrib} \\ & = & ((p \vee p) \vee q) \Leftrightarrow (\mathbf{F} \vee (p \vee q)) & \texttt{assoc}_\vee \\ & = & ((p \vee p) \vee q) \Leftrightarrow (p \vee q) & \texttt{ident}_\vee \\ & = & (p \vee q) \Leftrightarrow (p \vee q) & \texttt{idemp}_\vee \\ & = & \mathbf{T} & \texttt{const}_\Leftrightarrow \end{array}$$

(2) $(p \wedge q) \supset p$

$$
\begin{array}{rcll}
(p \wedge q) \supset p & = & ((p \wedge q) \Leftrightarrow \mathbf{F}) \vee p & \supset\texttt{-def} \\
& = & (((p \vee q) \Leftrightarrow (p \Leftrightarrow q)) \Leftrightarrow \mathbf{F}) \vee p & \wedge\texttt{-def} \\
& = & ((((p \vee q) \Leftrightarrow p) \Leftrightarrow q) \Leftrightarrow \mathbf{F}) \vee p & \texttt{assoc}_{\Leftrightarrow} \\
& = & ((((p \vee q) \Leftrightarrow p) \Leftrightarrow q) \vee p) \Leftrightarrow (\mathbf{F} \vee p) & \texttt{distrib} \\
& = & ((((p \vee q) \Leftrightarrow p) \Leftrightarrow q) \vee p) \Leftrightarrow p & \texttt{ident}_{\vee} \\
& = & ((((p \vee q) \Leftrightarrow p) \vee p) \Leftrightarrow (q \vee p)) \Leftrightarrow p & \texttt{distrib} \\
& = & ((((p \vee q) \vee p) \Leftrightarrow (p \vee p)) \Leftrightarrow (q \vee p)) \Leftrightarrow p & \texttt{distrib} \\
& = & ((((p \vee q) \vee p) \Leftrightarrow p) \Leftrightarrow (q \vee p)) \Leftrightarrow p & \texttt{idemp}_{\vee} \\
& = & ((((q \vee p) \vee p) \Leftrightarrow p) \Leftrightarrow (q \vee p)) \Leftrightarrow p & \texttt{comm}_{\vee} \\
& = & (((q \vee (p \vee p)) \Leftrightarrow p) \Leftrightarrow (q \vee p)) \Leftrightarrow p & \texttt{assoc}_{\vee} \\
& = & (((q \vee p) \Leftrightarrow p) \Leftrightarrow (q \vee p)) \Leftrightarrow p & \texttt{idemp}_{\vee} \\
& = & ((q \vee p) \Leftrightarrow p) \Leftrightarrow ((q \vee p) \Leftrightarrow p) & \texttt{assoc}_{\Leftrightarrow} \\
& = & \mathbf{T} & \texttt{const}_{\Leftrightarrow}
\end{array}
$$

(3) $(p \wedge q) \supset q$

$$
\begin{array}{rcll}
(p \wedge q) \supset p & = & (p \wedge q \Leftrightarrow \mathbf{F}) \vee q & \supset\texttt{-def} \\
& = & (((p \vee q) \Leftrightarrow (p \Leftrightarrow q)) \Leftrightarrow \mathbf{F}) \vee q & \wedge\texttt{-def} \\
& = & ((((p \vee q) \Leftrightarrow p) \Leftrightarrow q) \Leftrightarrow \mathbf{F}) \vee q & \texttt{assoc}_{\Leftrightarrow} \\
& = & ((((p \vee q) \Leftrightarrow p) \Leftrightarrow q) \vee q) \Leftrightarrow (\mathbf{F} \vee q) & \texttt{distrib} \\
& = & ((((p \vee q) \Leftrightarrow p) \Leftrightarrow q) \vee q) \Leftrightarrow q & \texttt{ident}_{\vee} \\
& = & ((((p \vee q) \Leftrightarrow p) \vee q) \Leftrightarrow (q \vee q)) \Leftrightarrow q & \texttt{distrib} \\
& = & ((((p \vee q) \Leftrightarrow p) \vee q) \Leftrightarrow q) \Leftrightarrow q & \texttt{ident}_{\vee} \\
& = & ((((p \vee q) \vee q) \Leftrightarrow (p \vee q)) \Leftrightarrow q) \Leftrightarrow q & \texttt{distrib} \\
& = & (((p \vee (q \vee q)) \Leftrightarrow (p \vee q)) \Leftrightarrow q) \Leftrightarrow q & \texttt{assoc}_{\vee} \\
& = & (((p \vee q) \Leftrightarrow (p \vee q)) \Leftrightarrow q) \Leftrightarrow q & \texttt{idemp}_{\vee} \\
& = & (\mathbf{T} \Leftrightarrow q) \Leftrightarrow q & \texttt{const}_{\Leftrightarrow} \\
& = & q \Leftrightarrow q & \texttt{ident}_{\Leftrightarrow} \\
& = & \mathbf{T} & \texttt{const}_{\Leftrightarrow}
\end{array}
$$

(4) $p \supset (q \supset p)$

$$
\begin{array}{rcll}
p \supset (q \supset p) & = & (p \Leftrightarrow \mathbf{F}) \vee (q \supset p) & \supset\texttt{-def} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((p \Leftrightarrow \mathbf{F}) \vee p) & \supset\texttt{-def} \\
& = & ((p \Leftrightarrow \mathbf{F}) \vee (p \Leftrightarrow \mathbf{F})) \vee p & \texttt{assoc}_{\vee} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee p & \texttt{idemp}_{\vee} \\
& = & (p \vee p) \Leftrightarrow (\mathbf{F} \vee p) & \texttt{distrib} \\
& = & p \Leftrightarrow (\mathbf{F} \vee p) & \texttt{idemp}_{\vee} \\
& = & p \Leftrightarrow p & \texttt{ident}_{\vee} \\
& = & \mathbf{T} & \texttt{const}_{\Leftrightarrow}
\end{array}
$$

(5) $\sim q \supset (q \supset p)$

$$
\begin{array}{rcll}
\sim q \supset (q \supset p) & = & (\sim q \Leftrightarrow \mathbf{F}) \vee (q \supset p) & \supset\texttt{-def} \\
& = & ((q \Leftrightarrow \mathbf{F}) \Leftrightarrow \mathbf{F}) \vee (q \supset p) & \sim\texttt{-def} \\
& = & ((q \Leftrightarrow \mathbf{F}) \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee p) & \supset\texttt{-def} \\
& = & (q \Leftrightarrow (\mathbf{F} \Leftrightarrow \mathbf{F})) \vee ((q \Leftrightarrow \mathbf{F}) \vee p) & \texttt{assoc}_{\vee} \\
& = & (q \Leftrightarrow \mathbf{T}) \vee ((q \Leftrightarrow \mathbf{F}) \vee p) & \texttt{const}_{\Leftrightarrow} \\
& = & q \vee ((q \Leftrightarrow \mathbf{F}) \vee p) & \texttt{ident}_{\Leftrightarrow} \\
& = & (q \vee (q \Leftrightarrow \mathbf{F})) \vee p & \texttt{assoc}_{\vee} \\
& = & ((q \vee q) \Leftrightarrow (q \vee \mathbf{F})) \vee q & \texttt{distrib} \\
& = & (q \Leftrightarrow (q \vee \mathbf{F})) \vee q & \texttt{idemp}_{\vee} \\
& = & (q \Leftrightarrow q) \vee q & \texttt{ident}_{\vee} \\
& = & \mathbf{T} \vee q & \texttt{const}_{\Leftrightarrow} \\
& = & \mathbf{T} & \texttt{ident}_{\Leftrightarrow}\texttt{-with}_{\vee}
\end{array}
$$

(6) $p \supset q \supset (\sim q \supset \sim p)$

$$
\begin{array}{rcll}
p \supset (q \supset (\sim q \supset \sim p)) & = & (p \Leftrightarrow \mathbf{F}) \vee (q \supset (\sim q \supset \sim p)) & \supset\texttt{-def} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee (\sim q \supset \sim p)) & \supset\texttt{-def} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee ((\sim q \Leftrightarrow \mathbf{F}) \vee \sim p)) & \supset\texttt{-def} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee (((q \Leftrightarrow \mathbf{F}) \Leftrightarrow \mathbf{F}) \vee \sim p)) & \sim\texttt{-def} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee (((q \Leftrightarrow \mathbf{F}) \Leftrightarrow \mathbf{F}) \vee (p \Leftrightarrow \mathbf{F}))) & \sim\texttt{-def} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow (\mathbf{F} \Leftrightarrow \mathbf{F})) \vee (p \Leftrightarrow \mathbf{F}))) & \texttt{assoc}_{\Leftrightarrow} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{T}) \vee (p \Leftrightarrow \mathbf{F}))) & \texttt{const}_{\Leftrightarrow} \\
& = & (p \Leftrightarrow \mathbf{F}) \vee ((q \Leftrightarrow \mathbf{F}) \vee (q \vee (p \Leftrightarrow \mathbf{F}))) & \texttt{ident}_{\Leftrightarrow} \\
& = & (p \vee p \vee q \vee q) \Leftrightarrow (p \vee p \vee q) \Leftrightarrow & \\
& & (p \vee q \vee q) \Leftrightarrow (p \vee q) \Leftrightarrow & \\
& & (p \vee q \vee q) \Leftrightarrow (p \vee q) \Leftrightarrow & \\
& & (q \vee q) \Leftrightarrow q & \texttt{distrib} \\
& = & (p \vee q) \Leftrightarrow (p \vee q) \Leftrightarrow (p \vee q) \Leftrightarrow (p \vee q) \Leftrightarrow & \\
& & (p \vee q) \Leftrightarrow (p \vee q) \Leftrightarrow q \Leftrightarrow q & \texttt{idemp}_{\vee} \\
& = & \mathbf{T} \Leftrightarrow \mathbf{T} \Leftrightarrow \mathbf{T} \Leftrightarrow \mathbf{T} & \texttt{const}_{\Leftrightarrow} \\
& = & \mathbf{T} \Leftrightarrow \mathbf{T} & \texttt{const}_{\Leftrightarrow} \\
& = & \mathbf{T} & \texttt{const}_{\Leftrightarrow}
\end{array}
$$

(7) $(p \vee p) \Leftrightarrow p$

$$
\begin{array}{rcll}
(p \vee p) \Leftrightarrow p & = & p \Leftrightarrow p & \texttt{idemp}_{\vee} \\
& = & \mathbf{T} & \texttt{const}_{\Leftrightarrow}
\end{array}
$$

3. $\langle \mathbb{Z}, =_5, +, * \rangle$ is a field.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Clearly, $=_5$ satisfies ref, sym, and trans, $+$ satisfies subst and functionality, and $*$ satisifes subst and functionality. By inspection, we see that $+$ satisfies assoc and comm, 0 is the identity element for $+$, and $+$ satisfies inv. By inspection, we see that $*$ satisfies assoc and comm, 1 is the identity element for $*$, and $*$ satisfies inv'. Furthermore, we see that $*$ satisfies Z. Finally, we see that $+$ and $*$ satisfy distrib.

4. Define $x < y \equiv (\exists z)(x + (z + \mathbf{1}) = y)$. We prove the seven axioms of discrete linear orders for $<$ from the Peano axioms.

   We assume that all of the axioms of integral domains have been proven from the Peano axioms.

   We first prove some useful lemmas:

   `lemma1`: $(\forall x, z)((x + z = x) \supset (z = \mathbf{0}))$

	$\mathbf{0} + z = \mathbf{0}$	`base`
$\supset$	$z + \mathbf{0} = \mathbf{0}$	`comm`$_+[\mathbf{0},z]$,`subst`
$\supset$	$z = \mathbf{0}$	`add-base`$[z]$,`subst`
	$(x + z = x) \supset (z = \mathbf{0})$	`ihyp`
	$x + \mathbf{1} + z = x + \mathbf{1}$	`step`
$\supset$	$x + z + \mathbf{1} = x + \mathbf{1}$	`comm`$_+[z,\mathbf{1}]$,`subst`
$\supset$	$x + z = x$	`injective`$[x + z,x]$
$\supset$	$z = \mathbf{0}$	`ihyp`

   `lemma2`: $(\forall x, a, y)((x + a = y) \supset ((x = y) \vee (x < y)))$

	$x + \mathbf{0} = y$	`base`
$\supset$	$x = y$	`add-base`$[x]$,`subst`
$\supset$	$(x = y) \vee (x < y)$	
	$(x + a = y) \supset ((x = y) \vee (x < y))$	`ihyp`
	$x + a + \mathbf{1} = y$	
$\equiv$	$x < y$	`lt-def`$[a]$
$\supset$	$(x = y) \vee (x < y)$	

   `lemma3`: $(\forall x, y)((x = y) \supset (x + \mathbf{1} = y + \mathbf{1}))$

	$x = y$	
$\wedge$	$x + (\mathbf{0} + \mathbf{1}) = (x + \mathbf{0}) + \mathbf{1}$	`add-step`$[x,\mathbf{0}]$
$\supset$	$x + (\mathbf{0} + \mathbf{1}) = (y + \mathbf{0}) + \mathbf{1}$	`subst`
$\supset$	$(x + \mathbf{0}) + \mathbf{1} = (y + \mathbf{0}) + \mathbf{1}$	`assoc`$_+[x,\mathbf{0},\mathbf{1}]$,`subst`
$\supset$	$x + \mathbf{1} = (y + \mathbf{0}) + \mathbf{1}$	`add-base`$[x]$,`subst`
$\supset$	$x + \mathbf{1} = y + \mathbf{1}$	`add-base`$[y]$,`subst`

   `lemma4`: $(\forall x, y, u, v)(((x < y) \wedge (u < v)) \supset (x + u < y + v))$

	$(x < y) \wedge (u < v)$	
$\equiv$	$(x + a + \mathbf{1} = y) \wedge (u < v)$	`lt-def`$[a]$
$\equiv$	$(x + a + \mathbf{1} = y) \wedge (u + b + \mathbf{1} = v)$	`lt-def`$[b]$
$\supset$	$(x + a + \mathbf{1} = y) \wedge (u + b + \mathbf{1} = v) \wedge (y + v = y + v)$	`ref`
$\supset$	$(u + b + \mathbf{1} = v) \wedge (x + a + \mathbf{1} + v = y + v)$	`subst`
$\supset$	$x + a + \mathbf{1} + u + b + \mathbf{1} = y + v$	`subst`
$\supset$	$x + u + a + \mathbf{1} + b + \mathbf{1} = y + v$	`comm`$_+[a + \mathbf{1},u]$,`subst`
$\equiv$	$x + u < y + v$	`lt-def`$[a + \mathbf{1} + b]$

`lt-asym`: $(\forall x, y)(x < y \supset \sim(y < x))$

	$\sim(x < y \supset \sim(y < x))$	by contradiction
$\equiv$	$\sim(\sim(x < y) \vee \sim(y < x))$	
$\equiv$	$\sim\sim(x < y) \wedge \sim\sim(y < x)$	
$\equiv$	$(x < y) \wedge (y < x)$	
$\equiv$	$(x + a + \mathbf{1} =) \wedge (y < x)$	`lt-def`$[a]$
$\equiv$	$(x + a + \mathbf{1} =) \wedge (y + b + \mathbf{1} = x)$	`lt-def`$[b]$
$\supset$	$x + a + \mathbf{1} + b + \mathbf{1} = x$	`subst`
$\supset$	$a + \mathbf{1} + b + \mathbf{1} = \mathbf{0}$	`lemma1`$[x, a + \mathbf{1} + b + \mathbf{1}]$
$\supset$	False	`non-surjective`$[a + \mathbf{1} + b]$
$\Rightarrow$	$x < y \supset \sim(y < x)$	

`lt-trans`: $(\forall x, y, z)((x < y \wedge y < z) \supset (x < z))$

	$(x < \mathbf{0}) \wedge (\mathbf{0} < z)$	`base`$[z]$
$\supset$	$x < \mathbf{0}$	
$\equiv$	$x + a + \mathbf{1} = \mathbf{0}$	`lt-def`$[a]$
$\supset$	False	`non-surjective`$[x + a]$
$\supset$	$x < z$	
	$((x < y) \wedge (y < z)) \supset (x < z)$	`ihyp`$[z]$
	$(x < y + \mathbf{1}) \wedge (y + \mathbf{1} < z)$	`step`$[z]$
$\equiv$	$(x + a + \mathbf{1} = y + \mathbf{1}) \wedge (y + \mathbf{1} + b + \mathbf{1} = z)$	`def-lt`$[a]$,`def-lt`$[b]$
$\equiv$	$(x + a + \mathbf{1} = y + \mathbf{1}) \wedge (y < z)$	`def-lt`$[\mathbf{1} + b]$
$\supset$	$(x + a = y) \wedge (y < z)$	`injective`$[x + a, y]$,`subst`
$\supset$	$((x = y) \vee (x < y)) \wedge (y < z)$	`lemma2`$[x, a, y]$
$\supset$	$((x = y) \wedge (y < z)) \vee ((x < y) \wedge (y < z))$	
$\supset$	$(x < z) \vee ((x < y) \wedge (y < z))$	`subst`
$\supset$	$(x < z) \vee (x < z)$	`ihyp`$[z]$
$\supset$	$x < z$	

`lt-linear`: $(\forall x, y)((x < y) \vee (y < x) \vee (x = y))$

		`base`$[x]$
		`base`$[y]$
	$\mathbf{0 = 0}$	`ref`
$\supset$	$(\mathbf{0 < 0}) \vee (\mathbf{0 < 0}) \vee \mathbf{0 = 0}$	
		`step`$[y]$
	$y + \mathbf{1} + \mathbf{0} = y + \mathbf{1}$	`add-base`$[y + \mathbf{1}]$
$\supset$	$\mathbf{0} + y + \mathbf{1} = y + \mathbf{1}$	`comm`$_+[y + \mathbf{1}, \mathbf{0}]$
$\equiv$	$\mathbf{0} < y + \mathbf{1}$	`lt-def`$[y]$
$\supset$	$(\mathbf{0} < y + \mathbf{1}) \vee (y + \mathbf{1} < \mathbf{0}) \vee (\mathbf{0} = y + \mathbf{1})$	

	$(x < y) \vee (y < x) \vee (x = y)$	`ihyp`$[x]$
		`step`$[x]$
	$(x < y) \vee (y < x) \vee (x = y)$	`ihyp`$[x]$
$\supset$	$(x + a + \mathbf{1} = y) \vee (y < x) \vee (x = y)$	`lt-def`$[a]$
$\supset$	$(x + a + \mathbf{1} + \mathbf{1} = y + \mathbf{1}) \vee (y < x) \vee (x = y)$	`lemma3`$[x + a + \mathbf{1}, y]$
$\supset$	$(x + \mathbf{1} + a + \mathbf{1} = y + \mathbf{1}) \vee (y < x) \vee (x = y)$	`comm`$_+[a, \mathbf{1}]$
$\supset$	$(x + \mathbf{1} < y + \mathbf{1}) \vee (y < x) \vee (x = y)$	`lt-def`$[a]$
$\supset$	$(x + \mathbf{1} < y + \mathbf{1}) \vee (y + b + \mathbf{1} = x) \vee (x = y)$	`lt-def`$[b]$
$\supset$	$(x + \mathbf{1} < y + \mathbf{1}) \vee (y + b + \mathbf{1} + \mathbf{1} = x + \mathbf{1}) \vee (x = y)$	`lemma3`$[y + b + \mathbf{1}, x]$
$\supset$	$(x + \mathbf{1} < y + \mathbf{1}) \vee (y + \mathbf{1} + \mathbf{1} + \mathbf{1} = x + \mathbf{1}) \vee (x = y)$	`comm`$_+[b, \mathbf{1}]$
$\supset$	$(x + \mathbf{1} < y + \mathbf{1}) \vee (y + \mathbf{1} < x + \mathbf{1}) \vee (x = y)$	`lt-def`$[b]$
$\supset$	$(x + \mathbf{1} < y + \mathbf{1}) \vee (y + \mathbf{1} < x + \mathbf{1}) \vee (x + \mathbf{1} = y + \mathbf{1})$	`lemma3`$[x, y]$

`lt-discrete`: $(\forall x, y) \sim ((x < y) \wedge (y < x + \mathbf{1}))$

	$\sim\sim((x < y) \wedge (y < x + \mathbf{1}))$	by contradiction
$\equiv$	$(x < y) \wedge (y < x + \mathbf{1})$	
$\equiv$	$(x + a + \mathbf{1} = y) \wedge (y < x + \mathbf{1})$	`lt-def`$[a]$
$\equiv$	$(x + a + \mathbf{1} = y) \wedge (y + b + \mathbf{1} = x + \mathbf{1})$	`lt-def`$[b]$
$\supset$	$x + a + \mathbf{1} + b + \mathbf{1} = x + \mathbf{1}$	`subst`
$\supset$	$x + a + \mathbf{1} + b = x$	`injective`$[x + a + \mathbf{1} + b, x]$
$\supset$	$a + \mathbf{1} + b = \mathbf{0}$	`lemma1`$[x, a + \mathbf{1} + b]$
$\supset$	$a + b + \mathbf{1} = \mathbf{0}$	`comm`$_+[Co, b]$
$\supset$	False	`non-surjective`$[a + b]$
$\Rightarrow$	$\sim((x < y) \wedge (y < x + \mathbf{1}))$	

`lt-0-1`: $\mathbf{0 < 1}$

	$(\mathbf{0 + 1}) + \mathbf{0} = \mathbf{0 + 1}$	`add-base`$[\mathbf{0 + 1}]$
$\supset$	$\mathbf{0} + (\mathbf{0 + 1}) = \mathbf{0 + 1}$	`comm`$_+[\mathbf{0 + 1}, \mathbf{0}]$,`subst`
$\supset$	$\mathbf{0} + (\mathbf{0 + 1}) = \mathbf{1 + 0}$	`comm`$_+[\mathbf{0}, \mathbf{1}]$,`subst`
$\supset$	$\mathbf{0} + (\mathbf{0 + 1}) = \mathbf{1}$	`add-base`$[\mathbf{1}]$,`subst`
$\equiv$	$\mathbf{0 < 1}$	`lt-def`$[\mathbf{0}]$

`lt-mono-+`: $(\forall x, y, z)((x < y) \supset (x + z < y + z))$

	$x < y$	`base`$[z]$
$\supset$	$x + \mathbf{0} < y$	`add-base`$[x]$,`subst`
$\supset$	$x + \mathbf{0} < y + \mathbf{0}$	`add-base`$[y]$,`subst`
	$(x < y) \supset (x + z < y + z)$	`ihyp`$[z]$
	$x < y$	`step`$[z]$
$\supset$	$x + z < y + z$	`ihyp`$[z]$
$\equiv$	$x + z + a + \mathbf{1} = y + z$	`def-lt`$[a]$
$\supset$	$x + z + a + \mathbf{1} + \mathbf{1} = y + z + \mathbf{1}$	`lemma3`$[x + z + a + \mathbf{1}, y + z]$
$\supset$	$x + z + \mathbf{1} + a + \mathbf{1} = y + z + \mathbf{1}$	`comm`$_+[a, \mathbf{1}]$,`subst`
$\equiv$	$x + z + \mathbf{1} < y + z + \mathbf{1}$	`lt-def`$[a]$

`lt-mono-*`: $(\forall x, y, z)(((\mathbf{0} < z) \wedge (x < y)) \supset (x * z < y * z))$

	$(\mathbf{0} < \mathbf{0}) \wedge (x < y)$	`base`$[z]$
$\supset$	$\mathbf{0} < \mathbf{0}$	
$\equiv$	$\mathbf{0} + a + \mathbf{1} = \mathbf{0}$	`lt-def`$[a]$
$\supset$	False	`non-surjective`$[\mathbf{0} + a]$
$\supset$	$x * \mathbf{0} < y * \mathbf{0}$	
	$((\mathbf{0} < z) \wedge (x < y)) \supset (x * z < y * z)$	`ihyp`$[z]$
	$(\mathbf{0} < z + \mathbf{1}) \wedge (x < y)$	`step`$[z]$
$\equiv$	$(\mathbf{0} + a + \mathbf{1} = z + \mathbf{1}) \wedge (x < y)$	`lt-def`$[a]$
$\supset$	$(\mathbf{0} + a = z) \wedge (x < y)$	`injective`$[\mathbf{0} + a, z]$
$\supset$	$((\mathbf{0} = z) \vee (\mathbf{0} < z)) \wedge (x < y)$	`lemma2`$[\mathbf{0}, a, z]$
$\supset$	$((\mathbf{0} = z) \wedge (x < y)) \vee ((\mathbf{0} < z) \wedge (x < y))$	
$\supset$	$((\mathbf{0} = z) \wedge (x < y)) \vee ((x < y) \wedge (x * z < y * z))$	`ihyp`$[z]$
$\supset$	$((\mathbf{0} = z) \wedge (x < y)) \vee ((x * z) + x < (y * z) + y)$	`lemma4`$[x, y, x * z, y * z]$
$\supset$	$((\mathbf{0} = z) \wedge (x < y)) \vee (x * (z + \mathbf{1}) < (y * z) + y)$	`mul-step`$[x, z]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (x < y)) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`mul-step`$[y, z]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (x + \mathbf{0} < y)) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`add-base`$[x]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (x + \mathbf{0} < y + \mathbf{0})) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`add-base`$[y]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (\mathbf{0} + x < y + \mathbf{0})) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`comm`$_+[x, \mathbf{0}]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (\mathbf{0} + x < \mathbf{0} + y)) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`comm`$_+[y, \mathbf{0}]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge ((x * \mathbf{0}) + x < \mathbf{0} + y)) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`mul-base`$[x]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge ((x * \mathbf{0}) + x < (y * \mathbf{0}) + y)) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`mul-base`$[y]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (x * (\mathbf{0} + \mathbf{1}) < (y * \mathbf{0}) + y)) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`mul-step`$[x, \mathbf{0}]$,`subst`
$\supset$	$((\mathbf{0} = z) \wedge (x * (\mathbf{0} + \mathbf{1}) < y * (\mathbf{0} + \mathbf{1}))) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`mul-step`$[y, \mathbf{0}]$,`subst`
$\supset$	$(x * (z + \mathbf{1}) < y * (z + \mathbf{1})) \vee (x * (z + \mathbf{1}) < y * (z + \mathbf{1}))$	`subst`
$\supset$	$x * (z + \mathbf{1}) < y * (z + \mathbf{1})$	