CS 474
Homework 4

Name: Adharsh Kamath NetID: ak128

<u>Problem 1</u>

Soln: A group is defined as a set S, along with a binary operation $\cdot : S \times S \to S$ and axioms:

1. $\forall a, b, c \,.\, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\forall a \,.\, ((a \cdot e) = a \wedge (e \cdot a) = a)$
3. $\forall a\, \exists b \,.\, ((b \cdot a) = e \wedge (a \cdot b) = e)$

where e is the special constant that is the identity element of the group.

Task 1:

$$G : \forall e' \,.\, ((\forall a \,.\, ((e \cdot a) = a \ \wedge (e' \cdot a) = a))$$
$$\implies (e = e'))$$

The first two axioms are in prenex normal form, and do not contain any existential quantifiers. Skolemizing the third axiom (by replacing $\exists b$ with a function $f(a)$), we get:

$$\forall a \,.\, (a \cdot f(a))$$
$$= e \wedge (a \cdot f(a))$$
$$= e$$

Simplifying the goal G, to prenex normal form:

$$\forall e' \, \forall a \,.\, ((a \cdot e') = a \ \wedge (e' \cdot a) = a) \implies (e = e')$$
$$\equiv \forall e' \, \neg(\forall a \,.\, ((a \cdot e') = a \ \wedge (e' \cdot a) = a))$$
$$\vee (e = e')$$
$$\equiv \forall e' \, (\exists a \,.\, \neg((a \cdot e') = a \ \wedge (e' \cdot a) = a))$$
$$\vee (e = e')$$

To show the validity of the goal, we need to show that the negation of the goal is unsatisfiable along with all the axioms.

$$\neg G \equiv \neg(\forall e' \, (\exists a \,.\, \neg((a \cdot e') = a \ \wedge (e' \cdot a) = a))$$
$$\vee (e = e'))$$

$$\equiv \exists e' \, \neg(\exists a \,.\, \neg((a \cdot e') = a \ \wedge (e' \cdot a) = a))$$
$$\wedge \neg(e = e')$$
$$\equiv \exists e' \, (\forall a \,.\, ((a \cdot e') = a \ \wedge (e' \cdot a) = a))$$
$$\wedge \neg(e = e')$$

Skolemizing (with a constant e'' since $\exists e'$ is the outermost existential quantifier), we get:

$$\forall a \,.\, ((a \cdot e'') = a \,\wedge\, (e'' \cdot a) = a \wedge \neg(e = e''))$$

Combining all the axioms, we have:

$$\forall a\,,b\,,c\,.\, (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$\forall a\,.\, ((a \cdot e) = a \wedge (e \cdot a) = a)$$
$$\forall a\,.\, ((a \cdot f(a))$$
$$= e \wedge (f(a) \cdot a) = e)$$
$$\forall a\,.\, ((a \cdot e'') = a \,\wedge\, (e'' \cdot a) = a \wedge \neg(e = e''))$$

Instantiating with depth-0 terms (e, e''), we get a large set (conjunction) of formulae :

$$(e \cdot e) \cdot e = e \cdot (e \cdot e)$$
$$(e \cdot e) \cdot e'' = e \cdot (e \cdot e'')$$
$$(e \cdot e'') \cdot e = e \cdot (e'' \cdot e)$$
$$(e \cdot e'') \cdot e'' = e \cdot (e'' \cdot e'')$$
$$(e'' \cdot e) \cdot e = e'' \cdot (e \cdot e)$$
$$(e'' \cdot e) \cdot e'' = e'' \cdot (e \cdot e'')$$
$$(e'' \cdot e'') \cdot e = e'' \cdot (e'' \cdot e)$$
$$(e'' \cdot e'') \cdot e'' = e'' \cdot (e'' \cdot e'')$$
$$(e \cdot e) = e \wedge (e \cdot e) = e$$
$$(e'' \cdot e) = e \wedge (e \cdot e'') = e$$
$$(e \cdot f(e))$$
$$= e \wedge (f(e) \cdot (e))$$
$$= e$$
$$(e'' \cdot f(e''))$$
$$= e \wedge (f(e'') \cdot (e''))$$
$$= e$$
$$(e \cdot e'') = e \wedge (e'' \cdot e) = e \wedge \neg(e = e'')$$
$$(e'' \cdot e'') = e'' \wedge (e'' \cdot e'') = e'' \wedge \neg(e = e'')$$

In this list, we can find two conjuncts that are contradictory:

$$(e \cdot e'') = e'' \wedge (e'' \cdot e) = e''$$
$$(e'' \cdot e) = e \wedge (e \cdot e'') = e \wedge \neg(e = e'')$$

Hence, there exists no model that satisfies all the formulae. Therefore, the goal G is valid.

The corresponding Z3 program is at the following URL: https://github.com/adharshkamath/logic-hw-4/blob/main/p1_1.py

Task 2: Given the skolemized set of axioms:

$$\forall a\,,b\,,c\,.\,(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$\forall a\,.\,((a \cdot e) = a \wedge (e \cdot a) = a)$$
$$\forall a\,.\,((f(a) \cdot a) = e \wedge (a \cdot f(a))$$
$$= e)$$

we can see that f is the inverse function. We can formulate the required goal as:

$$G:\ \forall a, b, c.(((a \cdot b = e) \wedge (b \cdot a = e))$$
$$\wedge((a \cdot c = e) \wedge (c \cdot a = e))$$
$$\implies (b = c))$$

Negating this goal and simplifying gives us:

$$\neg G:\ \exists a, b, c.(((a \cdot b = e) \wedge (b \cdot a = e))$$
$$\wedge((a \cdot c = e) \wedge (c \cdot a = e))$$
$$\wedge \neg(b = c))$$

Skolemizing (with constants a', b', c') gives us:

$$((a' \cdot b' = e) \wedge (b' \cdot a' = e))$$
$$\wedge((a' \cdot c' = e) \wedge (c' \cdot a' = e))$$
$$\wedge \neg(b' = c')$$

Instantiating the axioms with depth-0 terms (a', b', c', e), we get a long list (conjunction) of formulae. The full list is at the end of the document. Specifically, we can find four formulae that are not satisfiable together:

$$((b' \cdot a') \cdot c) == (b' \cdot (a' \cdot c))$$
$$(b' \cdot e) == b' \wedge (e \cdot b') == b'$$
$$(c' \cdot e) == c' \wedge (e \cdot c') == c'$$
$$(a' \cdot b') == e \wedge (b' \cdot a') == e \wedge (a' \cdot c') == e \wedge (c' \cdot a') == e \wedge \neg(b' = c')$$

Hence, there exists no model that can satisfy all the formulae. Therefore, the goal G is valid.

The Z3 program for this task is at the following URL: https://github.com/adharshkamath/logic-hw-4/blob/main/p1_pt2.py

An alternate proof using the formulation given in the lecture notes is at the end of the document. The alternate proof required using a depth-1 term for the instantiation of the axioms. The Z3 program for the alternate proof is at the following URL: https://github.com/adharshkamath/logic-hw-4/blob/main/p1_pt_alt.py

<u>Problem 2</u>
Soln:

(a)
The given formula φ

$$\varphi = y \leq x \wedge x \leq y \wedge f(y) = f(7) \wedge x \leq 5$$

contains terms from T_{UIF} and T_N (theory of UIF and theory of natural numbers).

Replacing $f(7)$ with $f(w)$, and adding $w = 7$ as an additional formula, we get:

$$\varphi' = y \leq x \wedge x \leq y \wedge x \leq 5 \wedge w = 7 \wedge f(y) = f(w)$$

The part of the formula in T_{UIF} :

$$F_{UIF} : f(y) = f(w)$$

and the part of the formula in T_N :

$$F_N : y \leq x \wedge x \leq y \wedge x \leq 5 \wedge w = 7$$

The conjunct $F_{UIF} \wedge F_N$ is $(T_{UIF} \cup T_N)$-equisatisfiable to φ.

(b)
The shared variables between F_{UIF} and F_N are:

$$V = \text{shared}(F_{UIF}, F_N) = \{y, w\}$$

The two possible equivalence relations and their arrangements are:

$$E_1 = \{\{y\}, \{w\}\}, \quad \alpha_1(E_1, V) : y = w$$
$$E_2 = \{\{y, w\}\}, \quad \alpha_2(E_2, V) : y \neq w$$

Simplifying F_N, we can write:

$$F_N = y \leq x \wedge x \leq y \wedge x \leq 5 \wedge w = 7$$
$$\equiv x = y \wedge x \leq 5 \wedge w = 7$$

We can see that F_N is satisfiable over natural numbers only under the arrangement α_2 (since $y \leq 5$ and $w = 7$). A satisfying model for F_N is: $\{x = 5, y = 5, w = 7\}$

We can see that F_{UIF} is satisfiable under this arrangement if f maps all natural numbers to a constant (since we need to satisfy $f(y) = f(w) \wedge y \neq w$). A satisfying model for F_{UIF} is: $\{y = 5, w = 7, (f(t) = 0 \text{ for any } t \in \mathbb{N})\}$.

From the above two models, we can derive a model for the original formula φ. Since y is the only shared variable that is present in the original formula, we need to make sure the y in the final model is consistent with above models we have found for the individual parts.

A satisfying model for φ is: $\{x = 5, y = 5, (f(t) = 0 \text{ for any } t \in \mathbb{N})\}$.

Problem 3
Soln:

(a)
The following is the least fixed point of the given function f:

$$\text{lfp}(f) = \{0, 2, 4, ...\} = \{2n \mid n \in \mathbb{N}\}$$

(b)
f is monotonic, if $A \subseteq B$ implies $f(A) \subseteq f(B)$.

Consider two sets A, B such that $A \subseteq B$. If x is an element of $f(A)$, then that means $x \in X$ and there exists a c such that $c \in \mathbb{N}$, c is prime and $cx \in A$. Since $A \subseteq B$, $cx \in B$. This means, $x \in f(B)$ (since c is prime and $cx \in B$).

Therefore, $f(A) \subseteq f(B)$.

Using the iterative method:

$$\begin{aligned}
X_0 &= \emptyset \\
X_1 &= f(X_0) = \{100\} \\
X_2 &= f(X_1) = \{100, 50, 20\} \\
X_3 &= f(X_2) = \{100, 50, 20, 25, 10, 4\} \\
X_4 &= f(X_3) = \{100, 50, 20, 25, 10, 4, 5, 2\} \\
X_5 &= f(X_4) = \{100, 50, 20, 25, 10, 4, 5, 2\}
\end{aligned}$$

We can see that $X_4 = X_5$, and hence the least fixed point is $\{100, 50, 20, 25, 10, 4, 5, 2\}$.

(c)
Informally, f "adds" 0 to a set, and removes 1 if it existed in the set. An operator is monotonic, if $A \subseteq B$ implies $f(A) \subseteq f(B)$. We can show monotonicity by that all elements of $f(A)$ are in $f(B)$ if all elements of A are in B.

Consider x such that $x \in f(A)$. This means, $x \in A \cup \{0\}$ and $x \neq 1$. Consider the following cases for any such x:

1. $x \in A$: In this case, $x \in A$, and hence $x \in B$. Since we know $x \neq 1$ (because $x \in f(A)$), $x \in f(B)$.

2. $x = 0 \wedge x \notin A$: In this case, $x \in f(B)$ since 0 is always added by f.

Therefore, $A \subseteq B$ implies $f(A) \subseteq f(B)$.

The least fixed point of f is $\{0\}$.

(d)

Informally, f "adds" 1 to a set, adds the double of every input element to the set, and removes the odd numbers from the input set. Consider sets A, B such that $A \subseteq B$, and $x \in f(A)$. Consider the following cases for any such x:

1. $x = 1$: In this case, $x \in f(B)$ since 1 is always added by f.

2. $x = 2n, n \in A$: In this case, $n \in B$, and hence $2n \in f(B)$. Therefore $x \in f(B)$.

Note that x cannot be an odd number (other than 1), since f removes all odd numbers from the input set. So the above cases are exhaustive.

Therefore, $A \subseteq B$ implies $f(A) \subseteq f(B)$.

The least fixed point of f is $\{1\} \cup \{2x \mid x \in \mathbb{N}\}$

Complete list of quantifier instantiations for Task 2 (Alternate proof):

$$((a' \cdot a') \cdot a') = (a' \cdot (a' \cdot a')),$$
$$((a' \cdot a') \cdot b') = (a' \cdot (a' \cdot b')), ((a' \cdot b') \cdot a') = (a' \cdot (b' \cdot a')),$$
$$((a' \cdot b') \cdot b') = (a' \cdot (b' \cdot b')), ((b' \cdot a') \cdot a') = (b' \cdot (a' \cdot a')),$$
$$((b' \cdot a') \cdot b') = (b' \cdot (a' \cdot b')), ((b' \cdot b') \cdot a') = (b' \cdot (b' \cdot a')),$$
$$((b' \cdot b') \cdot b') = (b' \cdot (b' \cdot b')), ((a' \cdot a') \cdot e) = (a' \cdot (a' \cdot e)),$$
$$((a' \cdot e) \cdot a') = (a' \cdot (e \cdot a')), ((a' \cdot e) \cdot e) = (a' \cdot (e \cdot e)),$$
$$((e \cdot a') \cdot a') = (e \cdot (a' \cdot a')), ((e \cdot a') \cdot e) = (e \cdot (a' \cdot e)),$$
$$((e \cdot e) \cdot a') = (e \cdot (e \cdot a')), ((e \cdot e) \cdot e) = (e \cdot (e \cdot e)),$$
$$((a' \cdot a') \cdot c') = (a' \cdot (a' \cdot c')), ((a' \cdot c') \cdot a') = (a' \cdot (c' \cdot a')),$$
$$((a' \cdot c') \cdot c') = (a' \cdot (c' \cdot c')), ((c' \cdot a') \cdot a') = (c' \cdot (a' \cdot a')),$$
$$((c' \cdot a') \cdot c') = (c' \cdot (a' \cdot c')), ((c' \cdot c') \cdot a') = (c' \cdot (c' \cdot a')),$$
$$((c' \cdot c') \cdot c') = (c' \cdot (c' \cdot c')), ((b' \cdot b') \cdot c') = (b' \cdot (b' \cdot c')),$$
$$((b' \cdot c') \cdot b') = (b' \cdot (c' \cdot b')), ((b' \cdot c') \cdot c') = (b' \cdot (c' \cdot c')),$$
$$((c' \cdot b') \cdot b') = (c' \cdot (b' \cdot b')), ((c' \cdot b') \cdot c') = (c' \cdot (b' \cdot c')),$$
$$((c' \cdot c') \cdot b') = (c' \cdot (c' \cdot b')), ((b' \cdot b') \cdot e) = (b' \cdot (b' \cdot e)),$$
$$((b' \cdot e) \cdot b') = (b' \cdot (e \cdot b')), ((b' \cdot e) \cdot e) = (b' \cdot (e \cdot e)),$$
$$((e \cdot b') \cdot b') = (e \cdot (b' \cdot b')), ((e \cdot b') \cdot e) = (e \cdot (b' \cdot e)),$$
$$((e \cdot e) \cdot b') = (e \cdot (e \cdot b')), ((c' \cdot c') \cdot e) = (c' \cdot (c' \cdot e)),$$
$$((c' \cdot e) \cdot c') = (c' \cdot (e \cdot c')), ((c' \cdot e) \cdot e) = (c' \cdot (e \cdot e)),$$
$$((e \cdot c') \cdot c') = (e \cdot (c' \cdot c')), ((e \cdot c') \cdot e) = (e \cdot (c' \cdot e)),$$
$$((e \cdot e) \cdot c') = (e \cdot (e \cdot c'))$$

$$((a' \cdot b') \cdot e) = (a' \cdot (b' \cdot e)),$$

$$((a' \cdot e) \cdot b') = (a' \cdot (e \cdot b')), ((e \cdot a') \cdot b') = (e \cdot (a' \cdot b')),$$

$$((e \cdot b') \cdot a') = (e \cdot (b' \cdot a')), ((b' \cdot a') \cdot e) = (b' \cdot (a' \cdot e)),$$

$$((b' \cdot e) \cdot a') = (b' \cdot (e \cdot a')), ((a' \cdot b') \cdot c') = (a' \cdot (b' \cdot c'))$$

$$((a' \cdot c') \cdot b') = (a' \cdot (c' \cdot b')), ((c' \cdot a') \cdot b') = (c' \cdot (a' \cdot b')),$$

$$((c' \cdot b') \cdot a') = (c' \cdot (b' \cdot a')), ((b' \cdot a') \cdot c') = (b' \cdot (a' \cdot c')),$$

$$((b' \cdot c') \cdot a') = (b' \cdot (c' \cdot a')), ((a' \cdot c') \cdot e) = (a' \cdot (c' \cdot e)),$$

$$((a' \cdot e) \cdot c') = (a' \cdot (e \cdot c')), ((e \cdot a') \cdot c') = (e \cdot (a' \cdot c')),$$

$$((e \cdot c') \cdot a') = (e \cdot (c' \cdot a')), ((c' \cdot a') \cdot e) = (c' \cdot (a' \cdot e)),$$

$$((c' \cdot e) \cdot a') = (c' \cdot (e \cdot a')), ((b' \cdot c') \cdot e) = (b' \cdot (c' \cdot e)),$$

$$((b' \cdot e) \cdot c') = (b' \cdot (e \cdot c')), ((e \cdot b') \cdot c') = (e \cdot (b' \cdot c')),$$

$$((e \cdot c') \cdot b') = (e \cdot (c' \cdot b')), ((c' \cdot b') \cdot e) = (c' \cdot (b' \cdot e)),$$

$$((c' \cdot e) \cdot b') = (c' \cdot (e \cdot b')), (a' \cdot f(a') = e) \wedge (f(a') \cdot a' = e)$$

$$(b' \cdot f(b') = e) \wedge (f(b') \cdot b' = e)(c' \cdot f(c') = e) \wedge (f(c') \cdot c' = e)$$

$$(e \cdot f(e)) = e \wedge (f(e) \cdot e) = e(a' \cdot e) = a' \wedge (e \cdot a') = a'$$

$$(b' \cdot e) = b' \wedge (e \cdot b') = b'(c' \cdot e) = c' \wedge (e \cdot c') = c'$$

$$(e \cdot e) = e \wedge (e \cdot e) = e$$

$$(a' \cdot b') = e \wedge (b' \cdot a') = e \wedge (a' \cdot c') = e \wedge (c' \cdot a') = e \wedge \neg(b' = c')$$

Solution for Task 2 (Alternate proof):

We can formulate the goal as

$$G: \ \forall a, b.(((a \cdot b = e) \wedge (b \cdot a = e))$$
$$\implies (b = f(a))$$
$$)$$

Negating this goal gives us:

$$\neg G: \ \exists a, b.(((a \cdot b = e) \wedge (b \cdot a = e))$$
$$\wedge \neg(b = f(a))$$
$$)$$

Skolemizing (with constants a', b') gives us:

$$((a' \cdot b' = e) \wedge (b' \cdot a' = e))$$
$$\wedge \neg(b' = f(a'))$$

Instantiating the axioms with depth-0 terms (a', b', e), we get a long list (conjunction) of formulae:

$$(a' \cdot a') \cdot a' = a' \cdot (a' \cdot a')$$
$$(a' \cdot a') \cdot b' = a' \cdot (a' \cdot b')$$
$$(a' \cdot b') \cdot a' = a' \cdot (b' \cdot a')$$
$$(a' \cdot b') \cdot b' = a' \cdot (b' \cdot b')$$
$$(b' \cdot a') \cdot a' = b' \cdot (a' \cdot a')$$
$$(b' \cdot a') \cdot b' = b' \cdot (a' \cdot b')$$
$$(b' \cdot b') \cdot a' = b' \cdot (b' \cdot a')$$
$$(b' \cdot b') \cdot b' = b' \cdot (b' \cdot b')$$
$$(a' \cdot a') \cdot e = a' \cdot (a' \cdot e)$$
$$(a' \cdot e) \cdot a' = a' \cdot (e \cdot a')$$
$$(a' \cdot e) \cdot e = a' \cdot (e \cdot e)$$
$$(e \cdot a') \cdot a' = e \cdot (a' \cdot a')$$
$$(e \cdot a') \cdot e = e \cdot (a' \cdot e)$$
$$(e \cdot e) \cdot a' = e \cdot (e \cdot a')$$
$$(e \cdot e) \cdot e = e \cdot (e \cdot e)$$
$$(b' \cdot b') \cdot e = b' \cdot (b' \cdot e)$$
$$(b' \cdot e) \cdot b' = b' \cdot (e \cdot b')$$
$$(b' \cdot e) \cdot e = b' \cdot (e \cdot e)$$
$$(e \cdot b') \cdot b' = e \cdot (b' \cdot b')$$
$$(e \cdot b') \cdot e = e \cdot (b' \cdot e)$$
$$(e \cdot e) \cdot b' = e \cdot (e \cdot b')$$
$$(a' \cdot b') \cdot e = a' \cdot (b' \cdot e)$$
$$(a' \cdot e) \cdot b' = a' \cdot (e \cdot b')$$
$$(e \cdot a') \cdot b' = e \cdot (a' \cdot b')$$
$$(e \cdot b') \cdot a' = e \cdot (b' \cdot a')$$
$$(b' \cdot a') \cdot e = b' \cdot (a' \cdot e)$$
$$(b' \cdot e) \cdot a' = b' \cdot (e \cdot a')$$
$$(a' \cdot e) = a' \wedge (e \cdot a') = a'$$
$$(b' \cdot e) = b' \wedge (e \cdot b') = b'$$
$$(e \cdot e) = e \wedge (e \cdot e) = e$$
$$(a' \cdot f(a'))$$
$$= e \wedge (f(a') \cdot a') = e$$
$$(b' \cdot f(b'))$$
$$= e \wedge (f(b') \cdot b') = e$$
$$(e \cdot f(e))$$
$$= e \wedge (f(e) \cdot e) = e$$

In this list, we can find two conjuncts that are contradictory:

$$(a' \cdot f(a'))$$
$$= e \wedge (f(a') \cdot a') = e$$
$$(b' \cdot f(b'))$$
$$= e \wedge (f(b') \cdot b') = e$$