Instructor: Leo Goldmakher

NAME: ______________________

University of Toronto Scarborough
Department of Computer and Mathematical Sciences

MATC01: GROUPS AND SYMMETRY

Problem Set 7 – due Monday, November 4th

INSTRUCTIONS:
To receive credit, you must turn this in during the first 5 minutes of lecture on the due date. Please print and attach this page as the first page of your submitted problem set.

PROBLEM	**MARK**
Staple	
Coverpage	
7.1	
7.2	
7.3	
7.4	
7.5	
7.6	
Total	

Please read the following statement and sign below:

I understand that I am not allowed to use the internet to assist (in any way) with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person.

SIGNATURE:______________________

Problem Set 7

7.1 Let Γ be a group, and pick any $a, b \in \Gamma$.

(a) Suppose that there exists an element $g \in \Gamma$ such that $ag = g$. Prove that a is the identity.

(b) Let $b\Gamma := \{bg : g \in \Gamma\}$. Prove that $b\Gamma = \Gamma$.

7.2 Recall that a magic square is a square array of integers (not necessarily distinct) such that each row, each column, and the two main diagonals have the same sum.

(a) What can you say about 2×2 magic squares? Come up with the strongest claim you can, and prove it.

(b) In class, we saw the 3×3 magic square

8	1	6
3	5	7
4	9	2

This magic square uses each of the numbers from 1 to 9 exactly once. Determine all 3×3 magic squares with this property. Prove that you've found all of them. [*Hint: what can you say about the central square?*]

7.3 (Courtesy of J. Lagarias.) Let S be any set with at least two elements. Define a binary operation on S by setting $ab = b$ for every $a, b \in S$.

(a) Prove that S is closed under this product, that associativity holds, and that one can get from any element of S to any other via the operation.

(b) Explain why S is not a group.

7.4 (Courtesy of N. Pflueger) A binary operation on a set S is said to be *left transitive* if it allows you to get from any one element to any other by left multiplication, i.e. if for any pair of elements $a, b \in S$ there exists $g \in S$ such that $ga = b$. Similarly, we say the operation is *right transitive* if there exists an $h \in S$ such that $ah = b$.

In problem 7.3 you saw a set with binary operation which was associative and right transitive, but not a group. Let S be a non-empty set with a binary operation (under which S is closed), which is associative and both left *and* right transitive. The goal of this exercise is to prove that S is a group under this operation. As usual, we will denote the binary operation as a product.

(a) If $ex = x$ for some elements $e, x \in S$, we say e is a *left identity for* x; similarly, if $xe = x$ we say e is a *right identity for* x. Prove that an element is a left identity for one element of S if and only if it is a left identity for *every* element of S. The same argument shows that the same holds for any right identity.

(b) Prove that S has a unique identity element. [*Hint: first show that a left identity exists; similarly, a right identity exists. Next, prove that given a left and a right identity, the two must be equal. Conclude.*]

(c) Deduce that S is a group under the given binary operation.

7.5 Let Γ be a group. Recall that we write $H \leq \Gamma$ to denote that H is a subgroup of Γ.

(a) Prove that $Z(\Gamma) \leq \Gamma$, where $Z(\Gamma) := \{g \in \Gamma : ag = ga \ \forall a \in \Gamma\}$.

(b) Prove that if $K \leq H$ and $H \leq \Gamma$, then $K \leq \Gamma$.

7.6 Given a group Γ, suppose H is a finite *subset* of Γ which is closed under the binary operation of Γ. (As usual, we will denote this operation as a product.) The goal of this exercise is to prove that H must be a subgroup of Γ.

(a) Carefully explain why associativity holds in H.

(b) Prove that the identity $e \in H$. [*Hint*: Let $n = |H|$, the order of H. For any $a \in H$ which is not the identity, consider the set $S = \{a, a^2, a^3, \ldots, a^{n+1}\}$. Why must S be a subset of H? Why must two elements of S be equal to each other? Deduce that $e \in S$, and therefore, $e \in H$.]

(c) Prove that for all $a \in H$, we have $a^{-1} \in H$ (where a^{-1} is the inverse of a in Γ).