Instructor: Leo Goldmakher

NAME: ______________________________

University of Toronto Scarborough
Department of Computer and Mathematical Sciences

MATC01: GROUPS AND SYMMETRY

Problem Set 10 – due Monday, November 29th

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	
10.1	
10.2	
10.3	
10.4	
10.5	
10.6	
10.7	
10.8	
10.9	
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 10

I recommend proceeding in order, as some problems are easier to solve using the results of prior problems.

10.1 Recall that the set $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ forms a group under addition: $[a] + [b] := [a+b]$. We now define a new binary operation, multiplication: $[a] \cdot [b] := [ab]$. For example, in $\mathbb{Z}/7\mathbb{Z}$ we have $[3] \cdot [4] = [5]$.

(a) Prove that $\mathbb{Z}/7\mathbb{Z} - \{[0]\}$ forms a group under multiplication. Why do we have to remove the element $[0]$?

(b) Find the smallest set S such that $\mathbb{Z}/8\mathbb{Z} - S$ forms a group under multiplication.

10.2 The goal of this exercise is to prove the following:

Theorem. *Suppose the order of a group Γ is a multiple of 3. Then Γ has an element of order 3.*

In fact, this statement holds with 3 replaced by any prime, but you don't need to prove this.

Proof. Let

$$A := \{(x, y, z) \in \Gamma^3 : xyz = e\}.$$

In words, A is the set of all *ordered* triples of elements of Γ whose product is the identity. Consider the function

$$\begin{array}{cccc} \sigma : & A & \longrightarrow & A \\ & (x, y, z) & \longmapsto & (z, x, y) \end{array}$$

Let A^σ denote the set of all fixed points of σ, i.e.

$$A^\sigma := \{a \in A : \sigma(a) = a\}.$$

Observe that A^σ is nonempty, since it contains the trivial fixed point (e, e, e).

(a) Prove that **if** there exists a nontrivial fixed point of σ, then Γ contains an element of order 3.

(b) Prove that $A - A^\sigma = \bigcup_{a \in A - A^\sigma} [a]_\sigma$, where $[a]_\sigma := \{f(a) : f \in \langle\sigma\rangle\}$. (Here $\langle\sigma\rangle$ denotes the subgroup of S_A generated by σ.)

(c) Prove that for all $a, b \in A$, either $[a]_\sigma = [b]_\sigma$ or $[a]_\sigma \cap [b]_\sigma = \emptyset$.

(d) Prove that $|A - A^\sigma|$ is a multiple of 3.

(e) Conclude the proof of the theorem. [*Hint: What can you say about $|A|$?*] □

10.3 The theorem above holds when 3 is replaced by any prime (you don't need to prove this). However, show by example that 3 cannot be replaced by an arbitrary integer. In other words, find a group Γ and a divisor d of $|\Gamma|$ such that Γ has no elements of order d.

10.4 Consider the following group presentation:

$$\Gamma = \langle \alpha, \beta \;:\; \alpha^3 = 1,\, \beta^3 = 1,\, \beta\alpha = \alpha^2\beta \rangle$$

(a) Express $\alpha^2\beta^5\alpha^{-2}\beta$ in the form $\alpha^m\beta^n$, where $0 \le m \le 2$ and $0 \le n \le 2$.

(b) Determine the order of Γ.

10.5 Given a group Γ, let $Z(\Gamma) = \{a \in \Gamma : ag = ga \text{ for every } g \in \Gamma\}$.

(a) Prove that $Z(\Gamma) \trianglelefteq \Gamma$.

(b) Suppose $\Gamma/Z(\Gamma)$ is cyclic. Prove that Γ is abelian. [*Hint: Prove that there exists* $g \in \Gamma$ *such that* $\Gamma = \bigcup_{n\in\mathbb{Z}} g^n Z(\Gamma)$. *Conclude.*]

10.6 Suppose that a non-trivial group Γ has no non-trivial proper subgroups.

(a) Prove that Γ is cyclic.

(b) Prove that Γ has finite order. [*Hint: Suppose* Γ *were infinite, and derive a contradiction.*]

(c) Prove that Γ has prime order. [*Hint: Say* $\Gamma = \langle g\rangle$ *and has order* n. *What can you say about* $\langle g^2\rangle$*?* $\langle g^3\rangle$*?*]

10.7 Suppose H and K are groups. Consider the set $H \times K$ under the binary operation defined by

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1h_2, k_1k_2).$$

(a) Prove that $H \times K$ is a group under this operation. If H and K are both finite, what is the order of $H \times K$?

(b) Prove that $(H \times \{e_K\}) \trianglelefteq (H \times K)$.

(c) Prove that $(H \times K)/(H \times \{e_K\}) \simeq K$. [*Hint: First prove that* $[(x, y)] = (H, y)$ *for any* $(x, y) \in H \times K$*.*]

10.8 Given Γ a group, recall that S_Γ denotes the group of all bijections from Γ to itself (under composition). Given $g \in \Gamma$, define the function

$$\begin{aligned} \phi_g : \Gamma &\longrightarrow \Gamma \\ a &\longmapsto ga \end{aligned}$$

Thus, we have a bunch of different functions ϕ_g, one for each $g \in \Gamma$.

(a) Prove that $\phi_g \in S_\Gamma$ for every $g \in \Gamma$.

(b) Let $\phi : \Gamma \to S_\Gamma$ be the function defined by $\phi(g) = \phi_g$. Prove that ϕ is an injective homomorphism.

(c) Deduce that any group Γ is isomorphic to a subgroup of S_Γ.

10.9 Given $k \in \mathbb{N}$, we denote $S_{\{1,2,\ldots,k\}}$ by S_k; this is usually called *the symmetric group on* k *letters.*

(a) Prove that $S_m \times S_n$ is isomorphic to a subgroup of S_{m+n}.

(b) Use part (a) to prove that $m!\,n! \,\big|\, (m + n)!$