Abstract algebra I

MATH2113

Due: 17th September 2025

1) Consider the following six functions:

$$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{1}{x}, \quad f_4(x) = \frac{1}{1-x}$$

$$f_5(x) = \frac{x-1}{x}, \quad f_6(x) = \frac{x}{x-1}.$$

In this exercise we will explicitly describe a correspondence between these functions and the elements of the set

$$S = \{(1), (12), (13), (23), (123), (132)\}.$$

(Recall that we may view this set as the collection of reorderings of the vertices of an equilateral triangle, with vertices initially labeled by 1, 2, and 3. Then (1) corresponds to no reordering, (12) switches the labels 1 and 2 (same idea for (13) and (23)), while (123) sends 1 to 2, 2 to 3, and 3 to 1 (same idea for (132)).)

(a) Apart from f_1, for which i's do we have $f_i(f_i(x)) = x$?

(b) Which elements in S correspond to the f_i's obtained in (a)? Note that we need a 1-1 correspondence, and that the choice is **not** unique.

(c) For any two **distinct** f_i, f_j obtained in (a), show that $f_i(f_j(x)) \neq f_j(f_i(x))$. Show that this is also true in S, based on the correspondence you gave in (b).

(d) Based again on the correspondence you gave in (b), which elements in S do the remaining f_i's correspond to?

2) Let n be an integer greater than 1. We denote the set

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\}$$

to be the set of integers modulo n, this is a group under the binary operation $+$ described in class. We define the *multiplicative* binary operation $\cdot$ on $\mathbb{Z}/n\mathbb{Z}$ in the usual sense. For example, if $n = 5$, then $2 \cdot 2 = 4 \equiv 4 \mod 5$, and $3 \cdot 4 = 12 \equiv 2 \mod 5$. For each of the following n, list the elements in $x \in \mathbb{Z}/n\mathbb{Z}$ such that we can find a $y \in \mathbb{Z}/n\mathbb{Z}$ satisfying $x \cdot y = 1$.

(a) $n = 5$;

(b) $n = 6$;

(c) $n = 8$;

(d) $n = 13$;

(e) $n = 30$.

(The elements of $\mathbb{Z}/n\mathbb{Z}$ are actually not the integers as we know it, but we do not go into the details here.)

3) The set of elements described in Question 2 for each n forms a group under multiplication and is denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$. Clearly 0 is not included in $(\mathbb{Z}/n\mathbb{Z})^\times$ and so this group contains at most $n-1$ elements.

   (a) For $x \in \mathbb{Z}/n\mathbb{Z}$, prove that $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if there exists integers a, b such that $ax + bn = 1$.

   (b) Prove that $(\mathbb{Z}/n\mathbb{Z})^\times$ has $n-1$ elements if and only if n is prime.

4) Let $(G, *)$ be a group, where $*$ denotes the binary operation.

   (a) Show that the identity element and the inverse element of every $x \in G$ are unique. *(Recall that the identity element is the element $e \in G$ satisfying $e * x = x * e = x$ for all $x \in G$, and that the inverse element of $x \in G$ is an element $y \in G$ satisfying $y * x = x * y = e$.)*

   (b) If G has at most four elements, show that for all $x, y \in G$, we have $x * y = y * x$. *(This is also true if G has five elements, and Question 1 is the counterexample when considering groups with six elements.)*

   (c) Show that if every element $x \in G$ satisfies $x * x = e$, then for all $x, y \in G$ we have $x * y = y * x$.

   (In (b) and (c) we are simply proving that G is an abelian group.)