Introduction to Algebra I HW1

B13902024 張沂魁

September 15, 2025

1. Consider the following six functions:

$$f_1(x) = x, \quad f_2(x) = 1-x, \quad f_3(x) = \tfrac{1}{x}, \quad f_4(x) = \tfrac{1}{1-x}, \quad f_5(x) = \tfrac{x-1}{x}, \quad f_6(x) = \tfrac{x}{x-1}.$$

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?

Solution:

(a) By direct computation, we know

$$f_1(f_1(x)) = x \quad f_2(f_2(x)) = x \quad f_3(f_3(x)) = x$$
$$f_4(f_4(x)) = \frac{x-1}{x} \quad f_5(f_5(x)) = \frac{1}{1-x} \quad f_6(f_6(x)) = x.$$

Hence, the i's we want to find are $2, 3, 6$.

(b) If we want to have a 1-1 correspondence between the elemetns in S and the f_i's, then we can let

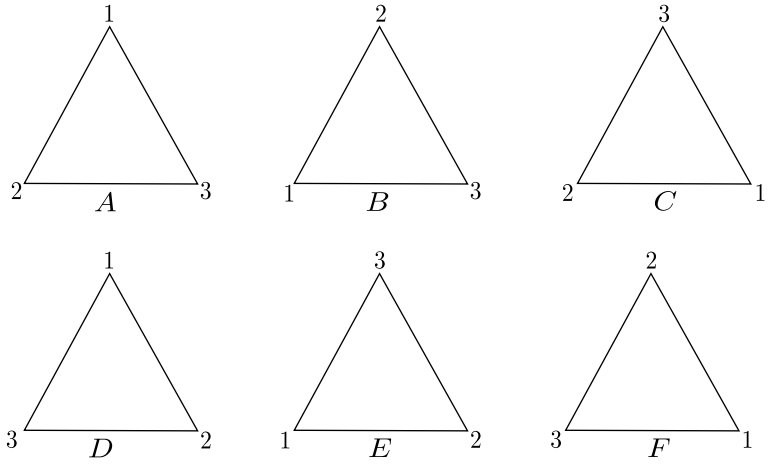
$$f_2 \leftrightarrow (12) \quad f_3 \leftrightarrow (13) \quad f_6 \leftrightarrow (23),$$

since $(12), (13), (23)$ are the operations that will be recovered after operating twice, so do f_2, f_3, f_6.

(c) First note that

$$\begin{array}{lll} f_2(f_3(x)) = \frac{x-1}{x} & f_2(f_6(x)) = \frac{1}{1-x} & f_3(f_6(x)) = \frac{x-1}{x} \\ f_3(f_2(x)) = \frac{1}{1-x} & f_6(f_2(x)) = \frac{x-1}{x} & f_6(f_3(x)) = \frac{1}{1-x} \end{array},$$

so $f_i(f_j(x)) \neq f_j(f_i(x))$ for all distinct i, j obtained in (a). Now we claim that this is also true in S. Suppose



Hence, we have

$$\begin{array}{lll} (13)((12)(A)) = E & (23)((12)(A)) = F & (23)((13)(A)) = E \\ (12)((13)(A)) = F & (12)((23)(A)) = E & (13)((23)(A)) = F \end{array},$$

where $(12)(A)$ means doing operation (12) on A, and the others are defined similarly. Hence, we know for distinct i, j obtained in (a), the correspondence given in (b) are also not commutative in S.

(d)

$$f_1 \leftrightarrow (1) \quad f_4 \leftrightarrow (123) \quad f_5 \leftrightarrow (132).$$

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

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

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 $2 \cdot 2 = 4 \equiv 4 \pmod 5$, and $3 \cdot 4 = 12 \equiv 2 \pmod 5$. 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.)
Solution: We use the result of (a) in 3. Hence, we just need to find the numbers coprime to n.

(a) $1, 2, 3, 4$.

(b) $1, 5$.

(c) $1, 3, 5, 7$.

(d) $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$.

(e) $1, 7, 11, 13, 17, 19, 23, 29$.

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 exist 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.

   Solution:

   (a) ($\Rightarrow$) If $[x] \in (\mathbb{Z}/n\mathbb{Z})^\times$, then there exists $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ s.t. $ax \equiv 1 \mod n$ since $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group. Thus, there exists some $a, b \in \mathbb{Z}$ s.t. $ax + bn = 1$.

   ($\Leftarrow$) If $ax + bn = 1$ for some $a, b \in \mathbb{Z}$, then $ax \equiv 1 \mod n$, and thus $[a], [x] \in (\mathbb{Z}/n\mathbb{Z})^\times$.

   (b) ($\Rightarrow$) If $(\mathbb{Z}/n\mathbb{Z})^\times$ has $n-1$ elements, then for all $[x] \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, we know there exists $a, b \in \mathbb{Z}$ s.t. $ax + bn = 1$ by (a). Note that

   $$\gcd(x, n) \mid ax + bn = 1,$$

   so $\gcd(x, n) = 1$, which means x is coprime to n for all $1 \leq x \leq n-1$. Thus, n is prime.

   ($\Leftarrow$) If n is prime, then we claim that for all $[x] \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, there exists $y \in \mathbb{Z}$ with $1 \leq y \leq n-1$ s.t. $xy \equiv 1 \mod n$. If not, since the remainder of xy modulo n cannot be 0 and 1, so there are $n-2$ choices, where y has $n-1$ choices. Thus, by Pigeonhole Principle we know there exists $y_1 \neq y_2$ with $1 \leq y_1 < y_2 \leq n-1$ s.t.

   $$xy_1 \equiv xy_2 \mod n \Leftrightarrow x(y_2 - y_1) \equiv 0 \mod n,$$

   but since n is prime, and $0 < y_2 - y_1 < n$, so $n \mid x$, but $x \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, so this is a contradiction. Now we know our claim is true, and it can be easily seen that for all $1 \leq y \leq n-1$, $[y] \in (\mathbb{Z}/n\mathbb{Z})^\times$, so $(\mathbb{Z}/n\mathbb{Z})^\times$ has $n-1$ elements.

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.

   (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.)
   Solution:

   (a) Suppose e, e' are both identity elements, then $e = e*e' = e'$, so the identity element is unique. Suppose y, y' are both inverse element of $x \in G$, then $y' = y * x * y' = y$.

   (b) Suppose the group contains e, a, b, c, where e is the identity element. Note that

   $$a * e = e * a \quad b * e = e * b \quad c * e = e * c \quad a * b = b * a.$$

   are trivial. Besides, we have to discuss two cases:

   Case 1: If two of $\{a, b, c\}$ are inverse of each other, WLOG says $a * b = e$. Then $c * c = e$ since the inverse of each element is unique. Also, we know $a * c$ cannot be e, a, c, since the inverse of a, c and the identity element is unique. So does, $c * a$. Thus $a * c = b = c * a$. Similarly we can show $b*c = a = c*b$. Hence, for all $x, y \in G$, we have $x*y = y*x$.

   Case 2: If $a * a = b * b = c * c = e$, then $a * b$ can not be a, b, e since the inverse of a, b and the identity element is unique. Hence, $a * b = c$, and similarly we can prove $b * a = c$. By same arguments, we know $a * c = c * a = b$ and $b * c = c * b = a$. Hence, for all $x, y \in G$, we have $x * y = y * x$.

   (c) If x or y is e, then $x * y = y * x$ is trivial. Also, if $x = y$, it is also trivial. Now suppose $x \neq y$ and $x, y \neq e$, then we know $x * y \neq x, y$. Thus, suppose $x * y = z$ for some $z \neq x, y$. Hence, we know

   $$x * y * z = z * z = e.$$

   Also, we have

   $$\begin{aligned} x = x * e = x * x * y * z = y * z, \\ y * x = y * y * z = z, \\ y = y * x * x = z * x. \end{aligned}$$

   By some computation, we know

   $$\begin{aligned} z * y = (z * z) * x = x = y * z, \\ x * z = (y * z) * z = y = z * x, \\ x * y = x * (z * x) = (x * z) * x = y * x. \end{aligned}$$

   Hence, we can conclude that for all $x, y \in G$, we must have $x * y = y * x$.