MATH 411 - Homework 1

Trung Dang

February 2023

Problem 1: Suppose $f, g : S \to S$ are functions which are both 1-1 and onto. Prove that:
(a) their composition $f \circ g : S \to S$
(b) the inverse function $f^{-1} : S \to S$
are also 1-1 and onto.

Proof. (a) First, we prove that $f \circ g$ is 1-1.
Assume the contrary, $\exists\ u \neq v$ such that:

$$f \circ g(u) = f \circ g(v) \tag{1}$$

, or

$$f(g(u)) = f(g(v)) \tag{2}$$

Since f is 1-1, $g(u) = g(v)$. And since g is also 1-1, $u = v$, is a contradiction.

Second, we prove that$f \circ g$ is onto.
Assume that there is an element $u \in S$ such that for no $v \in S$, $f(g(v)) = u$. Hence there must be an element w such that there is no $g(v) = w$. But since g is onto, this raises a contradiction.

In conclusion, $f \circ g$ is both 1-1 and onto

(b) We first prove that f^{-1} is 1-1. Assume that for some $u, v \in S$, $f^{-1}(u) = f^{-1}(v)$, then $f(u) = f(v)$, contradicting with f is 1-1.

Meanwhile, since for every $x \in S$, there is another element y such that $f(x) = y$, thus we have $f^{-1}(y) = x$. Therefore, f^{-1} is a surjection.

From the aforementioned claims, f^{-1} is a bijection. □

Problem 2: Which of the following are binary operations on the set $\mathbb{Z}$? Explain:
(a) $a \circ b = \mid a - b \mid$
(b) $a \circ b = \sqrt{\mid ab \mid}$
(c) $a \circ b = a^b$

Proof. (a) the operation is binary since it takes two inputs from $\mathbb{Z}$ and returns one output which is also in $\mathbb{Z}$

(b) the operation is NOT binary. While it takes 2 inputs, its output may not belong to $\mathbb{Z}$. For instance, $2 \circ 3 = \sqrt{6} \notin \mathbb{Z}$

(c) the operation is binary since it takes two inputs from $\mathbb{Z}$ and returns one output which is also in $\mathbb{Z}$ □

Problem 3: Let $(S, \circ)$ and $(T, \bullet)$ be sets with binary operations. A 1-1 and onto function $f : S \to T$ is called an *isomorphism* of binary operations if $f(a \circ b0 = f(a) \bullet f(b)$ for every $a, b \in S$
(a) Suppose $(S, \circ)$ and $(T, \bullet)$ are isomorphic and $(S, \circ)$ is a group. Show that $(T, \bullet)$ is also a group.
(b) Let $(\mathbb{R}_{>0}, \cdot)$be the set of positive numbers with binary operation multiplication. Show that $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$ are isomorphic binary operations.

Proof. (a) Because $(S, \circ)$ is a group, it must satisfy the three axioms of a group, namely:

- $$(a \circ b) \circ c = a \circ (b \circ c) \tag{3}$$
- existence of identity e
- existence of an inverse: $a \circ a^{-1} = a^{-1} \circ a = e$

We will prove the same axioms for $(T, \bullet)$.
Indeed, using (3), we have:

$$(f(a)\bullet f(b))\bullet f(c) = f(a\circ b)\bullet f(c) = f((a\circ b)\circ c) = f(a\circ(b\circ c)) = f(a)\bullet(f(b)\bullet f(c)) \tag{4}$$

So f is associative.

Moreover, since $f(a) \bullet f(e) = f(a \circ e) = f(a) = f(e \circ a) = f(e) \bullet f(a)$, $f(e)$ is the identity of $(T, \bullet)$.

And for all $f(a) \in T$, $f(a^{-1}) \bullet f(a) = f(a^{-1} \circ a) = f(e)$. Thus there exists an inverse in $(T, \bullet)$. So $(T, \bullet)$ satisfies three conditions of a group and is hence a group.

(b) Consider the function: $f : \mathbb{R} \to \mathbb{R}_{>0}$, mapping $x \mapsto e^x$. Then if we regard $(\mathbb{R}, +)$ as group S and $(\mathbb{R}_{>0}, \cdot)$ as T, then we have:

$$f(a + b) = f(a) \cdot f(b) \tag{5}$$

Thus they are isomorphic. □

Problem 4: Let 2^s be the power set of S and let $f : 2^s \to 2^s$ be the function that takes every subset $T \subseteq S$ to its complementary subset $S \setminus T$. Show that f is an isomorphism of binary operations $(2^s, \cup)$ and $(2^s, \cap)$

Proof. The problem is equivalent to

$$f(a \cup b) = f(a) \cap f(b)$$

, or

$$(a \cup b)^C = a^C \cap b^C$$

which is true by De Morgan's Law. $\square$

Problem 5: Prove that:
(a) In every group G and for every $a, b \in G$, the inverse element of ab is equal to $b^{-1}a^{-1}$
(b) In every group G, and for every $a \in G$, the inverse of a^{-1} is equal to a.

Proof. (a) Denote the identity element of the group as e, we have:

$$\begin{aligned}
&(ab)(ab)^{-1} = e \\
\Longleftrightarrow &a^{-1}(ab)(ab)^{-1} = a^{-1}e \\
\Longleftrightarrow &(a^{-1}a)b(ab)^{-1} = a^{-1} \\
\Longleftrightarrow &b^{-1}b(ab)^{-1} = b^{-1}a^{-1} \\
\Longleftrightarrow &(ab)^{-1} = b^{-1}a^{-1}
\end{aligned}$$

(b) By definition, $aa^{-1} = e = a^{-1}a$, so a^{-1} is an inverse of a and vice versa. We now prove the uniqueness of the inverse.

Indeed, assume $ab = e = ac$. Then using the associativity of group operations, we have $b = be = b(ac) = (ba)c = ec = c$. So, $b = c$, and a is therefore the unique inverse of a^{-1} $\square$

Problem 6: Suppose G is a group such that $(ab)^2 = a^2b^2$ for any $a, b \in G$. Prove that G is an Abelian group.

Proof. The problem can be re-written as, for any 2 numbers $a, b \in G$, the identity $ab = ba$ holds.
Indeed,

$$\begin{aligned}
&(ab)^2 = a^2b^2 \\
\Longleftrightarrow\ &abab = aabb \\
\Longleftrightarrow\ &a^{-1}(abab)b^{-1} = a^{-1}aabbb^{-1} \\
\Longleftrightarrow\ &(a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1}) \ \textbf{(associativity)} \\
\Longleftrightarrow\ &ba = ab \ \textbf{(inverse)}
\end{aligned}$$

Therefore G is an Abelian group. $\square$

Problem 7: (a) Prove that the following *cancellation law* holds in every group G: if $xa = xb$ then $a = b$
(b) Find 3 non-zero 2×2 matrices X,A,B such that $XA = XB$ but $A \neq B$
(c) Find 3 functions with domain $\mathbb{R}$ and range $\mathbb{R}$ such that $f \circ g = f \circ h$ but $g \neq h$

Proof. (a) Since $x, a, b \in G$, there exists an inverse x^{-1} of x. Therefore,

$$\begin{aligned} & xa = xb \\ \Longleftrightarrow & x^{-1}xa = x^{-1}xb \\ \Longleftrightarrow & a = b \ \textbf{(inverse)} \end{aligned}$$

(b) For instance: $X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 1 \\ 5 & 7 \end{bmatrix}$ .Then:

$$XA = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 5 & 7 \end{bmatrix} = XB \tag{6}$$

But $A \neq B$

(c) Take $g(x) = x, \forall x \in \mathbb{R}$, $h(x) = x + 2\pi, \forall x \in \mathbb{R}$. Choose:

$$\begin{aligned} & f(x) = \tan(x), \forall x \in \mathbb{R}, x \neq k\pi + \frac{\pi}{2}, \\ & f(x) = 0, \forall x = k\pi + \frac{\pi}{2} \end{aligned}$$

Then $f(g(x)) = f(h(x)), \forall x \in \mathbb{R}$, but $g(x) \neq h(x)$

□

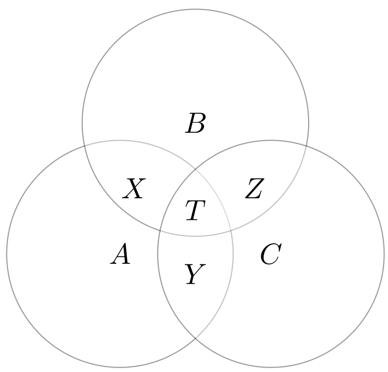
.

Problem 8: Consider the following operation with sets:

$$A \oplus B = (A \cup B) \setminus (A \cap B) \tag{7}$$

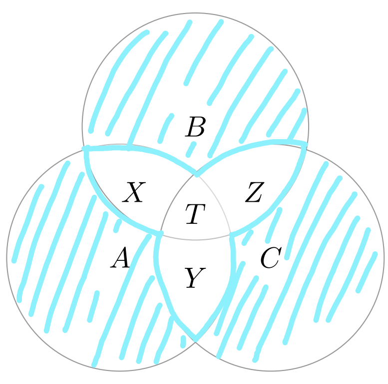
(a) Use Venn diagrams to prove that $\oplus$ satisfies associativity.
(b) Let S be an arbitrary set and let 2^S be its power set. Prove that $(2^S, \oplus)$ is a group. In particular, explain what is the identity and what is the inverse element.

Proof. (a)



For A, B, C, denote $A \cap B = X, B \cap C = Z, C \cap A = Y$, and $A \cap B \cap C = T$.

Then $(A \oplus B) \oplus C = (A \cup B \setminus X) \oplus C = (A \cup B \cup C) \setminus (X \cup Y \cup Z)$
And $A \oplus (B \oplus C) = A \oplus (B \cup C \setminus Z) = (A \cup B \cup C) \setminus (X \cup Y \cup Z)$.
In other words, both conditions are equivalent to the set of all elements in exactly one of A, B, C



Therefore $\oplus$ satisfies associativity.

(b) From problem (a) we know that the binary operation $\oplus$ is associative. Therefore, we are left to prove $(2^S, \oplus)$ has an identity and defines the inverse element.
For e to be the identity of 2^S, over operation $\oplus$, $\forall A \in 2^S$, $A \oplus e = A$. But we also know from (a) that $A \oplus B$ returns the elements in exactly one of A or B. Therefore, to preserve all the elements in A, $A \cap e = \emptyset$, and the empty set is the only element of 2^S that has no common element with any others. So $e = \emptyset$

Assume set A has an inverse B, then $A \oplus B = \emptyset$. This will only happens if $A \cup B = A \cap B$, or $B = A$. Thus, the inverse of an element is itself.

Since it has an identity and inverse, $(2^S, \oplus)$ is a group. $\square$

Problem 9: (a) Give an explicit algorithm to construct a bijection between the sets $\mathbb{Z}$ and $\mathbb{Q}$.
(b) Prove that there is no isomorphism between binary operations $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$

Proof. (a) Denote $\mathbb{Q}_{>0}, \mathbb{Q}_{<0}, \mathbb{Z}_{>0}, \mathbb{Z}_{<0}$ as the sets of positive and negative rational numbers, and the sets of positive and negative integers.
Since $\mathbb{Q} = \mathbb{Q}_{>0} \cup \{0\} \cup \mathbb{Q}_{<0}$ and $\mathbb{Z} = \mathbb{Z}_{>0} \cup \{0\} \cup \mathbb{Z}_{<0}$, it suffices to prove that there exists a bijection from $\mathbb{Q}_{>0} \to \mathbb{Z}_{>0}$, or $\mathbb{N}$, and similarly with their negative counterparts
We will create a table of natural coordinates, with column numbers as the numerator and rows representing denominators of fractions in $\mathbb{Q}_{>0}$ and assign to them a value in $\mathbb{Z}_{>0}$:

	1	2	3	4	5	...		
1	1	2	4	7	11			
2	3	5	8	12				
3	6	9	13					
4	10	14		⋰				
5	15							
⋮								

Similarly, we construct a bijection between $\mathbb{Z}_{<0}$ and $\mathbb{Q}_{<0}$. And mapping $0 \mapsto 0$, we have the desired construction.

(b) We have to prove the problem 2-fold: there is no isomorphism $\mathbb{Q} \to \mathbb{Z}$ and $\mathbb{Z} \to \mathbb{Q}$.

First Case: there is no isomorphism $\mathbb{Q} \to \mathbb{Z}$
Assume the contrary: there exists an isomorphism function $f : \mathbb{Q} \to \mathbb{Z}$. Then

$\exists q$ such that $f(q) = 1$. And since $f(q) = f(2 \times q/2) = 2f(q/2)$, we must have $f(q/2) = 1/2 \notin \mathbb{Z}$, a contradiction.

Second Case: there is no isomorphism $\mathbb{Z} \to \mathbb{Q}$
Let $f(1) = q$, then for all positive integer n, $f(n) = nf(1) = nq$. Meanwhile, $f(a+0) = f(a)+f(0)$, implying $f(0) = 0$. Thus, $f(-1+1) = f(-1)+f(1) = 0$, so $f(-1) = -q$. This implies that for all negative integers n, $f(n) = nq$. Thus, $f(n) = nf(1), \forall n \in \mathbb{Z}$, so the range of f is not $\mathbb{Q}$, a contradiction.

Therefore, there is no isomorphism between $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ $\square$