Solution - Abstract Algebra Assignments © BinaryPhi

Name: __________ **Assignment:** Number 2

Score: __________ **Last Edit:** May 26, 2022 PDT

Problem 1: Definitions

(a) Let "$\circ$" be the binary operation in the non-empty set S, and satisfies the following:

$$(a \circ b) \circ c = a \circ (b \circ c), \quad \forall a, b, c \in S.$$

Then, the algebraic system $\{S; \circ\}$ is called a **Semigroup** (S is a semigroup for short)

(b) If two elements e_1 and e_2 in the semigroup satisfy:

$$\begin{aligned} e_1 \circ a &= a, \\ a \circ e_2 &= a, \quad \forall a \in S \end{aligned}$$

e_1 is called the **Left Identity** of S, and e_2 is called the **Right Identity** of S.

If an element e in the semigroup satisfies:

$$e \circ a = a \circ e = a, \quad \forall a \in S,$$

e is called the **Identity Element** of S.

The semigroup that has Identity Element is called a **Monoid**.

(c) Assuming a monoid $\{S; \circ\}$ has the identity element e and an element $a \in S$, if:

$$\begin{aligned} a_1 \circ a &= e, \\ a \circ a_2 &= e, \quad \forall a_1, a_2 \in S \end{aligned}$$

a_1 is called the **Left Inverse** of a, and a_2 is called the **Right Inverse** of a.

If:

$$a_3 \circ a = a \circ a_3 = e, \quad \forall a_3 \in S,$$

a_3 is called the **Inverse Element** of a, and denoted by $a_3 = a^{-1}$.

(d) If every element in monoid $\{S; \circ\}$ is invertible, then S is called a **Group**.

(e) A group is a set S with an operation "$\circ$" that satisfies the following:

Closure: $\underline{\forall a, b \in S, \text{ we have } a \circ b \in S}$;

Associativity: $\underline{\forall a, b, c \in S, \text{ we have } (a \circ b) \circ c = a \circ (b \circ c)}$;

Identity: $\underline{\forall a \in S,\ \exists\ e \in S, \text{ so } e \circ a = a \circ e = a}$;

Invertibility: $\underline{\forall a \in S,\ \exists\ b \in S, \text{ so } b \circ a = a \circ b = e}$;

(f) Unilateral definition of the previous definition. Prove that a semigroup S is a group if it satisfies the following:

- $\forall a \in S,\ \exists\ b \in S$, so $b \circ a = e$;
- $\forall a \in S,\ \exists\ e \in S$, so $e \circ a = a$;

Invertibility: Assume $(a^{-1})^{-1}$ is a left inverse of a^{-1}: $(a^{-1})^{-1} \circ a^{-1} = e$, and $b \circ a = e$ could be rewritten as $a^{-1} \circ a = e$. Then,

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

Identity: By using the inverse property and the semigroup, we have:

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

(g) Interesting Question: Does the previous conclusions still hold if the semigroup has a left inverse and a right identity:

- $\forall a \in S,\ \exists\ a^{-1} \in S$, so $a^{-1} \circ a = e$;
- $\forall a \in S,\ \exists\ e \in S$, so $a \circ e = a$.

No: Assuming a semigroup with operation $a \circ b = a \cdot \sqrt{b^2} = a|b|$ with an identity element e. For any element m, $m \circ e = m$. However, for instance, for a nagetive m, we have $e \circ m = e|m| \neq m$. Thus, although the right identity exists in this scenario, the left identity doesn't exist.

No: Let $G = \left\{ \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \,\middle|\, x, y \in \mathbb{Q}, x \neq 0 \right\}$.

Because $\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x_1 & y_1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} xx_1 & xy_1 \\ 0 & 0 \end{smallmatrix}\right)$, G is a semigroup with a left identity $e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Because $\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x^{-1} & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = e$, $\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)$ has a right inverse.

However, for $y \neq 0$, $\left(\begin{smallmatrix} x_1 & y_1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \neq e$ ($x_1 x = 1$ and $x_1 y = 0$ contradict).

(h) Let the operation "$\circ$" in an algebraic system be commutative, the group $\{S; \circ\}$ is called the **Abelian Group** or **Commutative Group**.

(i) Prove that the operation "$\circ$" in group $\mathbb{G}$ is left(right) **Cancellative**:

$$\begin{aligned} \forall a, b, c \in \mathbb{G},\ a \circ b = a \circ c &\implies b = c \\ b \circ a = c \circ a &\implies b = c. \end{aligned}$$

Since $\mathbb{G}$ is a group, we have $a^{-1} \in \mathbb{G}$. By multiplying a^{-1} to the left of both sides of $a \circ b = a \circ c$, we have:

$$\begin{aligned} a^{-1} \circ (a \circ b) &= a^{-1} \circ (a \circ c) \\ (a^{-1} \circ a) \circ b &= (a^{-1} \circ a) \circ c \\ \therefore b &= c. \end{aligned}$$

It is the same for the proof of right cancellation law.

(j) The number of elements in group $\mathbb{G}$ is called the **Order** of $\mathbb{G}$, denoted by $|\mathbb{G}|$.

If $|\mathbb{G}|$ is finite, we call $\mathbb{G}$ a **Finite Group**. If $|\mathbb{G}|$ has infinite order, we call $\mathbb{G}$ a **Infinite Group**.

(k) Assuming the group $\mathbb{G}$ has an operation (multiplication or addtion) and a is an element of $\mathbb{G}$, if $\forall k \in \mathbb{N}$, $a^k \neq 1 (\neq e)$ or $ka \neq 0 (\neq e)$, we call the order of element a is **Infinite**. If $\exists\ k \in N$, $a^k = e$ or $ka = 0$, the order of element a is $\min\{k \in \mathbb{N} \mid a^k = e(ka = 0)\}$.

Problem 2: Prove:

1) There is only one inverse element of any element a in group $\mathbb{G}$.

Assuming a_1 and a_2 are two inverse elements of element a, we have

$$a_1 \circ a = e = a_2 \circ a.$$

According to the right cancellation law, $a_1 = a_2$.

2) For a group $\mathbb{G}$, $\forall a, b \in \mathbb{G}$, equations $a \circ x = b$ and $x \circ a = b$ have one and only one solution.

Since $\mathbb{G}$ is a group, we have $a^{-1} \in \mathbb{G}$.

Due to the closure property of group, we have $a^{-1} \circ b \in \mathbb{G}$, which is the(a) solution of $a \circ x = b$.

If x_1 and x_2 are both the solutions of $a \circ x = b$, we have $a \circ x_1 = b$ and $a \circ x_2 = b$, thus $a \circ x_1 = a \circ x_2$.

According to the right cancellation law, $x_1 = x_2$.

3) If $\forall a, b \in S$ for which S is a semigroup, S is a group if $a \circ x = b,\ x \circ a = b$ both have solutions.

Clossure:

Satisfied because S is a semigroup.

Associativity:

Satisfied because S is a semigroup.

Identity:

Since $x \circ a = a$ has solution in S, denoted by $e_a \circ a = a$.

$\forall c \in S$, $a \circ x = c$ has a solution denoted by d, which means:

$$a \circ d = c$$
$$e_a \circ (a \circ d) = (e_a \circ a) \circ d = a \circ d = \underline{c = e_a \circ c}$$

Invertibility:

Since $x \circ a = e_a$ has solution in S, the solution is the left inverse of a.

Problem 3: Check if the following options are semigroups, monoids, or groups?

1) In $\mathbb{Z}$, $a \circ b = a - b$;

Association Law Fails. Not a semigroup.

2) In $\mathbb{Z}$, $a \circ b = a + b + ab$;

Association Law:

$$(a \circ b) \circ c = (a + b + ab) + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc;$$
$$a \circ (b \circ c) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + ac + bc + abc;$$
$$\therefore (a \circ b) \circ c = a \circ (b \circ c)$$

Thus, the binary operation has associative property.

Identity Element:

$$e \circ b = e + b + eb \Longrightarrow e = 0,\ 0 \circ b = 0 + b + 0b = b;$$

Thus, for any element in $\mathbb{Z}$, there exists an identity element 0.

Inverse Element:

$$i \circ b = i + b + ib \Longrightarrow i = -1,\ (-1) \circ b = (-1) + b + (-1)b = -1;$$

Thus, for $i = -1$, the inverse element doesn't exist.

Therefore, $\{G; \circ\}$ is a monoid (with commutative binary operation).

3) In $\mathbb{Z}$, $a \circ b = a + b - ab$;

Association Law: ✓

$$(a \circ b) \circ c = a + b + c - ab - ac - bc + abc = a \circ (b \circ c);$$

Identity Element: ✓

$$e \circ b = e + b - eb \Longrightarrow e = 0,\ 0 \circ b = 0 + b - 0b = b;$$

Inverse Element:

$$i \circ b = i + b - ib \Longrightarrow i = 1,\ 1 \circ b = 1 + b - 1b = 1;$$

Thus, for $i = 1$, the inverse element doesn't exist.

Therefore, $\{G; \circ\}$ is a monoid (with commutative binary operation).

Problem 4: Define operation "$\circ$" in $S = \{x \mid x \in \mathbb{R}, x \neq -1\}$: $a \circ b = a + b + ab$. Prove that S is a group with respect to the operation "$\circ$". Then, solve equation $2 \circ x \circ 3 = 7$.

<ins>Association Law:</ins>

$$(a \circ b) \circ c = a + b + c + ab + ac + bc + abc = a \circ (b \circ c)$$

Thus, the binary operation has associative property.

<ins>Identity Element:</ins>

$$e \circ b = e + b + eb \Longrightarrow e = 0,\ 0 \circ b = 0 + b + 0b = b;$$

Thus, for any element in $\mathbb{Z}$, there exists an identity element 0.

<ins>Inverse Element:</ins>

Because $a \neq -1$, we have:

$$a \circ \frac{-a}{1+a} = a + \frac{-a}{1+a} + a\,\frac{-a}{1+a} = \frac{a(1+a) - a - a^2}{1+a} = \frac{a + a^2 - a - a^2}{1+a}$$

$$= 0$$

Thus, the inverse always exists.

Therefore, $\{G; \circ\}$ is a commutative group.

In addition, $2 \circ x \circ 3 = 7 \Longrightarrow$

$$x = \frac{-2}{1+2} \circ 7 \circ \frac{-3}{1+3}$$

$$= \frac{-2}{3} \circ 7 \circ \frac{-3}{4}$$

$$= \frac{-2}{3} + 7 + \frac{-3}{4} + \frac{-2}{3} \cdot 7 + \frac{-2}{3} \cdot \frac{-3}{4} + 7 \cdot \frac{-3}{4} + \frac{-2}{3} \cdot 7 \cdot \frac{-3}{4}$$

$$= \frac{1}{3}$$

Problem 5: Prove:

$\mathbb{G}$ is an Abelian Group if the order of every non-identity element is 2.

Assuming e is the identity element, we have:

$$\forall a \in \mathbb{G},\ a^2 = e \Longrightarrow a^{-1} = a.$$

Thus,

$$\forall a, b \in \mathbb{G}, ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Therefore, $\mathbb{G}$ is an Abelian Group (Commutative Group).

Problem 6: Assuming M is a monoid, $m \in M$. Define another multiplication rule "$\circ$": $a \circ b = amb$.

Prove that M is a semigroup with respect to "$\circ$".

When is M a monoid with respect to "$\circ$"?

Suppose $a, b, c \in M$, then we have:

$$\begin{aligned} (a \circ b) \circ c &= (amb) \circ c = ambmc \\ a \circ (b \circ c) &= a \circ (bmc) = ambmc \\ \therefore (a \circ b) \circ c &= a \circ (b \circ c) \end{aligned}$$

Thus, M is a semigroup.

Then, assuming 1 is the identity element of M and e is the identity element of $\{M; \circ\}$, then we have:

$$\begin{aligned} e \circ 1 = 1 = em1 = em \\ 1 \circ e = 1 = 1me = me \end{aligned}$$

Thus, m is invertible and $e = m^{-1}$. Then:

$$\begin{aligned} e \circ b = m^{-1}mb = b \\ b \circ e = bmm^{-1} = b \end{aligned}$$

Therefore, $\{M; \circ\}$ is a monoid when and only when m is invertible.

Problem 7: Assuming M is a monoid with an identity element e. It is said that the element a of M is invertible if there exists an element a^{-1} that satisfies $a^{-1}a = aa^{-1} = e$.

Prove the following statements:

1) If $a, b, c \in M$ and $ab = ca = e$, then a is invertible and $a^{-1} = b = c$.

We have:

$$ab = ca = e \Longrightarrow c(ab) = c(e) = c = b = eb = (ca)b;$$

So that, we have

$$ab = ba = e \Longrightarrow a^{-1} = b = c.$$

2) If $a \in M$ is invertible then $b = a^{-1}$m, when and only when $aba = a,\ ab^2a = e$.

$$ab^2a = e = (ab^2)a = a(b^2a)$$

Thus, a is invertible and $a^{-1} = ab^2 = b^2a$.

Then, because $aba = a$, we have:

$$a^{-1}aba = a^{-1}a \Longrightarrow ba = e \Longrightarrow a^{-1} = b.$$

3) The sufficient prerequisite of G, the subset of M, being a group is that every element in G is invertible and for all $g_1, g_2 \in G$, we have $g_1^{-1}g_2 \in G$.

$\Longrightarrow$: If G is a group, then every element g of G is invertible and every inverse of the element $g^{-1} \in G$. Then, we have: $\forall g_1, g_2 \in G \Longrightarrow g_1^{-1}g_2 \in G$.

$\Longleftarrow$: If $g \in G$ and g is invertible and $g_1, g_2 \in G$, $g_1^{-1}g_2 \in G \Longrightarrow (g_1^{-1})^{-1}g_2 = g_1, g_2 \in G$. Additionally, when $g_1 = g_2 = g \Longrightarrow g_1^{-1}g_2 = e \in G$, and $g_1^{-1} = g_1^{-1}e \in G$.

4) All invertible elements in M is a group.

Suppose the set of all invertible elements in M is U. It is apparent that every element of U is invertible. Assuming $g_1, g_2 \in G$, then:

$$(g_1^{-1}g_2)(g_2^{-1}g_1) = (g_2^{-1}g_1)(g_1^{-1}g_2) = e.$$

Therefore, $g_1^{-1}g_2 \in U \Longrightarrow U$ is a group.