Solutions: Homework 1

January 17, 2020

Problem 1. Let $\star$ be the binary operation on $\mathbb{Z}$ defined by $a \star b = a - b$. Is $\star$ commutative? Is it associative?

Proof. It is not commutative because $1 \star 2 = -1$ while $2 \star 1 = 1$, hence $1 \star 2 \neq 2 \star 1$. It is not associative because $(a \star b) \star c = (a - b) - c = a - b - c$ while $a \star (b \star c) = a - (b - c) = a - b + c$ and hence $(a \star b) \star c \neq a \star (b \star c)$ unless $c = 0$. □

Problem 2. Let $\star$ be the binary operation on $\mathbb{Z}^+$ defined by $a \star b = 2^{ab}$. Is $\star$ commutative? Is it associative?

Proof. It is commutative because $a \star b = 2^{ab} = 2^{ba} = b \star a$, because $ab = ba$. To check for associativity, let us look at $a \star (b \star c) = a \star 2^{bc} = 2^{a2^{bc}}$ and $(a \star b) \star c = 2^{ab} \star c = 2^{c2^{ba}}$. If $a = b = 1$ and $c = 4$, we have $1 \star (1 \star 4) = 2^{2^4} = 2^{16}$, while $(1 \star 1) \star 4 = 2^8$, and they are not equal. So $\star$ is not associative. □

Problem 3. Let H be the subset of $M_2(\mathbb{R})$ consisting of matrices of the form

$$H = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} | a, b \in \mathbb{R} \right\}.$$

(a) Is H closed under matrix addition?
(b) Is H closed under matrix multiplication?

Proof. (a) We want to prove that if A and B are two matrices in H, then $A + B$ is also in H. Let $A = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$ with $a_1, b_1, a_2, b_2 \in \mathbb{R}$. Then

$$A + B = \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix}$$

which clearly lies in H. So H is closed under matrix addition.
(b) We want to prove that if A and B are two matrices in H, then AB is also in H. Let $A = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$ with $a_1, b_1, a_2, b_2 \in \mathbb{R}$. Then

$$AB = \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + b_1a_2) \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

which clearly lies in H. So H is closed under matrix multiplication. □

Problem 4. Either prove the statement or give a counterexample. *Every commutative binary operation on a set having just two elements is associative.*

Proof. This statement is false. Consider the following table:

$\star$	a	b
a	b	a
b	a	a

This binary operation is obviously commutative, as $a \star b = b \star a$, but not associative as $(a \star a) \star b = b \star b = a$, while $a \star (a \star b) = a \star a = b$. □

In problems 5, 6 and 7, determine whether or not ϕ is an isomorphism of binary structures. If it is not an isomorphism, why not?

Problem 5. $(\mathbb{Z}, +)$ with $(\mathbb{Z}, +)$ where $\phi(n) = -n$ for all $n \in \mathbb{Z}$.

Proof. $\phi(n) = \phi(m)$ implies that $-n = -m$ and hence $n = m$. So ϕ is one-to-one. For any $n \in \mathbb{Z}, \phi(-n) = n$, hence it is also onto. So ϕ is a bijection.
For $n, m \in (\mathbb{Z}, +), \phi(n+m) = -(n+m) = -n-m = \phi(n)+\phi(m)$. So it is an isomorphism. □

Problem 6. $(\mathbb{Z}, +)$ with $(\mathbb{Z}, +)$ where $\phi(n) = 2n$ for all $n \in \mathbb{Z}$.

Proof. ϕ is not onto as there does not exist $n \in \mathbb{Z}$ such that $\phi(n) = 1$. So it is not bijective, and hence not an isomorphism. □

Problem 7. $(M_2(\mathbb{R}), .)$ with $(\mathbb{R}, .)$ where $\phi(A)$ is the determinant of the matrix A.

Proof. $\phi\left(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right) = \det\left(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right) = 0 = \det\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right) = \phi\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right)$. So ϕ is not injective, hence not bijective, and hence not an isomorphism. □

Problem 8. Consider the binary operation $\star$ on $\mathbb{Z}$ defined by $a \star b = ab$. Decide whether $(\mathbb{Z}, \star)$ is a group. If not, which axioms fail?

Proof. Integer multiplication is clearly associative, hence $\mathcal{G}_1$ axiom holds. For any $a \in \mathbb{Z}, 1 \star a = a \star 1 = a$, hence 1 clearly acts as the identity in $(\mathbb{Z}, \star)$ and hence $\mathcal{G}_2$ axiom also holds. $\mathcal{G}_3$ axiom fails because not every element has an inverse, for example there is no $a \in \mathbb{Z}$ such that $0 \star a = 1$, so 0 has no inverse. So $(\mathbb{Z}, \star)$ is not a group. □

Problem 9. Let n be a positive integer and let $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$.
(a) Show that $(n\mathbb{Z}, +)$ is a group.
(b) Show that $(n\mathbb{Z}, +)$ is isomorphic to $(\mathbb{Z}, +)$.

Proof. (a) $+$ is associative. So $\mathcal{G}_1$ axiom holds. $0 + nm = nm + 0 = nm$ for all $nm \in n\mathbb{Z}$. So 0 is the identity, hence $\mathcal{G}_2$ axiom holds. For any $nm \in n\mathbb{Z}, nm + n(-m) = n(-m) + nm = 0$, so $\mathcal{G}_3$ axiom also holds. So $(n\mathbb{Z}, +)$ is a group.
(b) Define the map $\phi : (n\mathbb{Z}, +) \to (\mathbb{Z}, +)$ by $\phi(a) = \frac{a}{n}$. Note that this makes sense because as a is in $n\mathbb{Z}, n$ divides a and hence $\frac{a}{n}$ is an integer. $\phi(a) = \phi(b)$ implies that $\frac{a}{n} = \frac{b}{n}$, hence $a = b$ and so ϕ is one-to-one. For any $k \in \mathbb{Z}, \phi(nk) = k$, hence ϕ is also onto. So ϕ is a bijection. Now, $\phi(a + b) = \frac{a+b}{n} = \frac{a}{n} + \frac{b}{n} = \phi(a) + \phi(b)$. So ϕ is an isomorphism. □

Problem 10. Give a table for a binary operation on the set $\{e, a, b\}$ of three elements satisfying axioms $\mathcal{G}_2$ and $\mathcal{G}_3$ but not axiom $\mathcal{G}_1$.

Proof. We shall choose e as our identity and a and b to be the inverses of each other, i.e. $a \star b = b \star a = e$. So $\star$ satsifies $\mathcal{G}_2$ and $\mathcal{G}_3$.

$\star$	e	a	b
e	e	a	b
a	a	a	e
b	b	e	b

Now, $(a \star a) \star b = a \star b = e$, while $a \star (a \star b) = a \star e = a$. So $\star$ is not associative, hence $\mathcal{G}_1$ fails. □

Problem 11. Show that if G is a group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a \star a = e$.

Proof. This is equivalent to proving that if G has an even number of elements, then there exists an $a \neq e$ in G such that the inverse of a is itself. We prove this by contradiction. Suppose that for all $a \neq e$ in G, the inverse of a is not a. Then, pairing together all elements other than e with its inverse gives us an even number of elements. Counting e, this implies that G has an odd number of elements. This contradicts our hypothesis that G has an even number of elements. □

Problem 12. Show that every group G with identity e such that $x \star x = e$ for all $x \in G$ is abelian.

Proof. Let a, b be any two elements in G. Then $(a \star b) \star (a \star b) = e$ by our hypothesis on G. By associativity, we have

$$((a \star b) \star a) \star b = e$$

Then

$$(((a \star b) \star a) \star b) \star b = e \star b = b$$

Again, by associativity, we have

$$((a \star b) \star a) \star (b \star b) = b$$

Since $b \star b = e$, we have

$$(a \star b) \star a = b$$

Then

$$((a \star b) \star a) \star a = b \star a$$

Again, by associativity, we have

$$(a \star b) \star (a \star a) = b \star a$$

Since $a \star a = e$, we have

$$a \star b = b \star a$$

So G is abelian. □