HW 2

Charles Liu
Elementary Modern Algebra - Dr. Ben Clark
January 25th

---

1. Determine if each of the given functions are binary operations. If a given function is a binary operation, determine if the binary operation is associative and commutative.

(a) $a - b$ for positive integers a, b.

Theorem. $a - b$ for positive integers a, b is *NOT* a binary operation.

Proof.
BWOC, assume that $a - b$ is a binary operation. Then it must map from $\mathbb{Z}^+$ to $\mathbb{Z}^+$, as $a, b \in \mathbb{Z}^+$. However, if $b > a$, then $a - b < 0$, and thus, $a - b \notin \mathbb{Z}^+$, a contradiction. Therefore, $a - b$ is *not* a binary operation.

(b) AB for invertible n by n matrices A, B.

Theorem. AB for invertible n by n matrices A, B is a binary operation.

Proof.
Since A, B are invertible n by n matrices, we want to show AB is also an invertible n by n matrix.
If A, B are invertible, then A^{-1} and B^{-1} must exist. Since $(AB) \cdot (B^{-1}A^{-1}) = e$ and $B^{-1}A^{-1}$ exists, AB must be invertible. Since A, B are both n by n, there product must also be n by n.
As such, AB is a binary operation.

Theorem. The binary operation AB for invertible n by n matrices A, B is associative.

Proof.
Assume there is three invertible n by n matrices A, B, C. We want to show that $(AB)C = A(BC)$.
Assume $(AB)C = D$, where D is a n by n matrix. Let $a_{ij}, b_{ij}, c_{ij}, d_{ij}$ denote the element at the ith row and jth column of A, B, C, D respectively.
Since $(AB)C = D$, $(a_{ij} \cdot b_{ji}) \cdot c_{ij} = d_ij$ by definition of matrix multiplication.

For $A(BC) = E$, where E is a n by n matrix. Let $a_{ij} \cdot \underbrace{(b_{ji} \cdot c_{ij})}_{ji\text{th element of } BC} = d_ij$.

Thus, $(AB)C = A(BC) = D$, and the operation AB is associative.

Theorem. AB for invertible n by n matrices A, B is *NOT* commutative.

Proof.

Assume $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix}$.

We can see that

$$AB = \begin{bmatrix} 1 \cdot 2 & 3 \cdot 1 \\ 2 \cdot 3 & 4 \cdot 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 6 & 4 \end{bmatrix}$$

We can also solve that

$$BA = \begin{bmatrix} 2 \cdot 1 & 1 \cdot 3 \\ 3 \cdot 1 & 4 \cdot 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}$$

Since $AB \neq BA$, the binary operation AB is *not* commutative.

(c) a/b for rational a, b.

Theorem. a/b is *NOT* a binary operation for rational a, b.

Proof.

Let a, b be rational. Assume $b = 0$. We get that $a/b = a/0$ which is undefined, and not a rational number.

Therefore, a/b is *NOT* a binary operation

(d) $|a||b|$ for complex numbers, a, b.

Theorem. $|a||b|$ for complex numbers, a, b is a binary operation.

Proof.

Let $a, b \in \mathbb{C}$. The magnitude of a complex number must always be a real number. Thus, $|a||b| \in \mathbb{R}$. Since real numbers are a subset of complex numbers, $|a||b| \in \mathbb{C}$.

Thus, $|a||b|$ is a binary operation.

---

2. Determine if the set H is a subgroup of the given group G under the same binary operation as G. Prove or provide a reason why it isn't.

(a) $H = \{3n \mid n \in Z\}$ where $G = (\mathbb{Z}, +)$.

Theorem. $H = \{3n \mid n \in Z\}$ where $G = (\mathbb{Z}, +)$ is a subgroup.

Proof.

We will use the one-step subgroup test.

1. $H \neq \emptyset$

Take $n = 0$. H must contain the identity element 0, and is thus not an empty set.

2. For $a \in H, a^{-1} \in H$.

We know that $a = 3n$. Since $a - a = 3n - 3n = e$, a^{-1} exists and is $-a$. Since $-a = -3n = 3k$ where $k = -n$, $-a = a^{-1} \in H$.

3. For $a, b \in H, ab^{-1} \in H$

If $a, b^{-1} \in H$, then $a = 3n_1 \in H$ and $b^{-1} = 3n_2 \in H$. This means that $ab^{-1} = 3n_1 n_2 = 3n_3 \in H$ where $n_3 = n_1 n_2$.

Since H is nonempty and $ab^{-1} \in H$, H is a subgroup of G.

(b) $H = \{1, 2, 5\}$ where $G = (\mathbb{Z}^6, +)$.

Theorem. $H = \{1, 2, 5\}$ where $G = (\mathbb{Z}^6, +)$ is *NOT* a subgroup.

Proof.

By way of contradiction, assume that H is a subgroup of G. This means that for $a, b \in H$, $ab \in H$.
If $a = 1$ and $b = 2$, $a + b \pmod 6 = 3 \pmod 6 = 3 \notin H$, a contradiction.
Thus, $H = \{1, 2, 5\}$ is *not* a subgroup of G.

(c) $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ where G is 2 by 2 real coefficient matrices under addition.

Theorem. $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ is a subgroup of G.

Proof.

We will use the two-step subgroup test.

1. $H \neq \emptyset$

Assume $a, b, c, d = 0$. We get that the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = e \in H$. As such, H is nonempty.

2. For $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \in H$

Since $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = e, a^{-1}$ exists and is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

Since $-a, -b, -c, -d \in \mathbb{Z}, a^{-1} \in H$.

As H is nonempty and any element in H's inverse is also in H, H is a subgroup of G.

---

3. Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Theorem. A group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Proof.

By the Socks and Shoes theorem, we can solve that $(ab)^{-1} = b^{-1}a^{-1}$. If G is abelian, elements in G are commutative, and $b^{-1}a^{-1} = a^{-1}b^{-1}$.
Thus, if G is abelian, then $(ab)^{-1} = a^{-1}b^{-1}$.

If $(ab)^{-1} = a^{-1}b^{-1}$, then $(ab)^{-1} = (ba)^{-1}$ by the Socks and Shoes theorem. Since in groups, inverses are a one-to-one operation, $ab = ba$, and thus the group is abelian.

Therefore, a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$.

---

4. Prove that the center of a group G is a subgroup of G.

Theorem. The center of a group G is a subgroup of G.

Proof.

Let H be the center of a group G. By definition, this means that $H = \{h \mid hg = gh\}$ where $h \in H, g \in G$.
We will use the one step subgroup test.

1. $H \neq \emptyset$

Since $eg = ge, e \in H$ so H is nonempty.

2. If $a \in H, a^{-1} \in H$

Since $a \in G, a^{-1}$ must exist as G is a group. Since $a \in H$,

$$\begin{aligned} ag &= ga \\ \implies a^{-1}aga^{-1} &= a^{-1}gaa^{-1} \\ \implies ga^{-1} &= a^{-1}g \end{aligned}$$

which means $a^{-1} \in H$.

3. For $a, b \in H, ab^{-1} \in H$.

If $a, b \in H$, then $ag = ga$ and $b^{-1}g = gb^{-1}$.
We can see that

$$\begin{aligned} b^{-1}g &= gb^{-1} \\ \implies ab^{-1}g &= agb^{-1} = (ag)b^{-1} \\ \implies ab^{-1}g &= gab^{-1} \end{aligned}$$

Thus, $ab^{-1} \in H$.

Since $H \neq \emptyset$ and $ab^{-1} \in H$, H is a subgroup. As such, the center of a subgroup G is a subgroup of G.

---

5. Prove that no group is the union of two proper subgroups. Does the statement remain true if we instead consider 3 proper subgroups?

Theorem. No group is the union of two proper subgroups.

Proof.

By way of contradiction, let G be a group that is the union of two proper subgroups H_1, H_2. By definition of proper subgroups, there must exist $h_1 \in H_1$ where $h_1 \notin H_2$ since H_2 is proper. Likewise, there must exist $h_2 \in H_2$ where $h_2 \notin H_1$ since H_1 is proper. Since $h_1, h_2 \in G$, by definition of groups, $h_1h_2 \in G$. Since $H_1 \cup H_2 = G$, either $h_1h_2 \in H_1$ or $h_1h_2 \in H_2$ (by definition of union).

Case 1: $h_1h_2 \in H_1$

If $h_1h_2 \in H_1$, since $h_1^{-1} \in H_1, h_1h_1^{-1}h_2 = h_2 \in H_1$, a contradiction. Thus, $h_1h_2 \notin H_1$.

Case 2: $h_1h_2 \in H_2$

Likewise, if $h_1h_2 \in H_2$, since $h_2^{-1} \in H_2, h_1h_2h_2^{-1} = h_1 \in H_2$, a contradiction. Thus, $h_1h_2 \notin H_2$.

Since $h_1h_2 \notin H_1$ and $h_1h_2 \notin H_2$ although h_1h_2 must be in H_1 or H_2, this is a contradiction. Therefore, G can not be the union of two proper subgroups.

Theorem. A group *CAN* be the union of three proper subgroups

Proof.

Assume a group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$.

We can find three subgroups, $H_1 = \{(0,0)(0,1)\}, H_2 = \{(0,0), (1,0)\}$, and $H_3 = \{(0,0)(1,1)\}$ where $H_1 \cup H_2 \cup H_3$.

Thus, a group *can* be the union of three proper subgroups.