Math 100A | | **Ray Tsai**
A02 5:00PM - 5:50PM | **Homework 0** | **A16848188**
Castellano-Macias | **Source Consulted: Textbook, Lecture, Discussion** | **Professor McKernan**

Question 1.1.1. Let S be a set having an operation $*$ which assigns an element $a * b$ of S for any $A, B \in S$. Let us assume that the following two rules hold:

1. If a, b are any objects in S, then $a * b = a$.
2. If a, b are any objects in S, then $a * b = b * a$.

Show that S can only have at most one object.

Proof. Suppose for the sake of contradiction that S has more than one object. Let $a, b \in S$ be two distinct objects. By rule one, $a * b = a$ and $b * a = b$, contradicting rule 2's statement that $a * b = b * a$. Therefore, S has at most one object. $\square$

Question 1.1.2. Let S be the set of all integers $0, \pm 1, \pm 2, \dots, \pm n, \dots$. For a, b in S define $*$ by $a * b = a - b$. Verify the following:

(a) $a * b \neq b * a$ unless $a = b$.

Proof. True. Let $a, b \in S$ such that $a \neq b$. Then $a + a \neq b + b$, and so $a * b = a - b \neq b - a = b * a$. □

(b) $(a * b) * c \neq a * (b * c)$ in general. Under what condition on a, b, c is $(a * b) * c = a * (b * c)$?

Proof. True. Let $a, b, c \in S$.

$$(a * b) * c = (a - b) - c = a - b - c \neq a - b + c = a - (b - c) = a * (b * c).$$

Suppose that $(a * b) * c = a * (b * c)$.

$$\begin{aligned} (a * b) * c &= a * (b * c) \\ a - b - c &= a - b + c \\ c &= 0. \end{aligned}$$

Only when $c = 0$ is $(a * b) * c = a * (b * c)$. □

(c) The integer 0 has the property that $a * 0 = a$ for every a in S.

Proof. True. $a * 0 = a - 0 = a$. □

(d) For a in S, $a * a = 0$.

Proof. True. $a * a = a - a = 0$. □

Question 2.1.1. Determine if the following sets G with the operation indicated form a group. If not, point out which of the group axioms fail.

(a) $G =$ the set of all integers, $a * b = a - b$.

Proof. Fails the associative property. Let $a, b, c \in \mathbb{Z}$.

$$a * (b * c) = a - (b - c) = a - b + c \neq (a - b) - c = (a * b) * c$$

□

(b) $G =$ the set of all integers, $a * b = a + b + ab$.

Proof. Fails the inverse property. Let $a, b \in \mathbb{Z}$. Since $a * 0 = 0 * a = a$, we know the identity element of G is 0. Let $a = 1$. Since $a * b = b * a = 1 + b + b = 1 + 2b = 0$ has no integer solutions, $(G, *)$ does not fulfill the inverse property. □

(c) $G =$ the set of non-negative integers, $a * b = a + b$.

Proof. Fails the inverse property. We know the identity element $e \in G$ is 0, as $s + 0 = 0 + s = s$ for any $s \in G$. For $a, b \in G$ such that $a \neq 0$, since $a + b > 0$, any positive element in G has no inverse. □

(d) $G =$ the set of all rational numbers $\neq -1$, $a * b = a + b + ab$.

Proof. $(G, *)$ forms a group. Let $a, b, c \in G$.

We first prove the closed property. We know $a + b + ab \in \mathbb{Q}$. Suppose for the sake of contradiction that $a + b + ab = -1$. Rearranged, we get $(a + 1)b = -(a + 1)$. Since $a \neq -1$, we cancel $(a + 1)$ from each side and get $b = -1$, contradiction. Therefore, $a + b + ab \in G$.

The associative property is met, as

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a * (b * c).\end{aligned}$$

Since $a * 0 = 0 * a = a$, $e = 0 \in G$ is the identity element.

Finally, we show the inverse property. Let $b = \frac{-a}{a+1}$. Since

$$a * b = b * a = a + \frac{-a}{a+1} + a \cdot \frac{-a}{a+1} = \frac{a^2 + a - a - a^2}{a+1} = 0,$$

for all $a \in G$, a has an inverse $b = \frac{-a}{a+1} \in G$.

Since all four properties are met, G with $*$ form a group. □

(e) $G =$ the set of all rational numbers with denominator divisible by 5 (written so that numerators and denominator are relatively prime), $a * b = a + b$.

Proof. Fails the identity property. Suppose for the sake of contradiction that there exists $e \in G$ such that $a * e = a + e = a$. Then $e = 0$. However, $0 \notin G$, as the numerator 0 is not relatively prime to any integer denominators divisible by 5, contradiction. $\square$

(f) G is the set having more than one element, $a * b = a$ for all $a, b \in G$.

Proof. Fails the identity property. Let $a, e \in G$ be two distinct elements. Suppose for the sake of contradiction that e is the identity element. We then have $e * a = e \neq a$, contradiction. $\square$

Question 2.1.2. In the group G defined in Example 6, show that the set $H = \{T_{a,b} \,|\, a = \pm 1, b \text{ any real }\}$ forms a group under the $*$ of G.

Proof. We prove all four properties of a group.

Closed property: Let $T_{a,b}, T_{c,d} \in H$. We then have

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}.$$

Since $ac = \pm 1$ and $ad + b \in \mathbb{R}$, $f * g \in H$.

Associative property: Let $f, g, h \in H$. Since all three functions are $\mathbb{R} \to \mathbb{R}$, we get $(f * g) * h = f * (g * h)$ by lemma 1.3.1 in Herstein.

Identity property: For all $T_{a,b} \in H$, we have $T_{1,0}$ such that

$$T_{a,b} * T_{1,0} = T_{a,b},$$
$$T_{1,0} * T_{a,b} = T_{a,b},$$

and thus G has an identity element $T_{1,0}$ under $*$.

Inverse property: For all $T_{a,b} \in H$, we have $T_{a,-a^{-1}b} \in H$, such that

$$T_{a,b} * T_{a,a^{-1}b} = T_{a^2,a \cdot a^{-1}b+b} = T_{1,0}$$
$$T_{a,a^{-1}b * T_{a,b}} = T_{a^2,a^{-1}b \cdot a+b} = T_{1,0}.$$

Since all four properties are fulfilled, H forms a group under the $*$ of G. ☐

Question 2.1.5. in Example 9, prove that $g * f = f * g^{-1}$, and that G is a group, is non-abelian, and is order of 8.

Proof. We restate that $S = \{(x, y) \in \mathbb{R}^2\}$, $f, g \in A(S)$ such that $f(x, y) = (-x, y)$ and $g(x, y) = (-y, x)$, and $G = \{f^i g^j \mid i = 0, 1; j = 0, 1, 2, 3\}$. Note that since f is a reflection and g is a 90° rotation, both $f^k = f^{(k \mod 2)}$ and $g^l = g^{(l \mod 4)}$ are in G, for $k, l \in \mathbb{Z}$. And also note that $g^4 = f^2 =$ identity mapping e.

We first prove that $g * f = f * g^{-1}$. We first note that since $e = g^4$, $g^{-1} = g^3 = (y, -x)$. On the left-hand side of the statement, we have

$$(g * f)(x, y) = g(f(x, y)) = g(-x, y) = (-y, -x).$$

On the right-hand side, we have

$$(f * g^{-1})(x, y) = f(g^3(x, y)) = f(y, -x) = (-y, -x).$$

Thus, we have $g * f = f * g^{-1} = (-y, -x)$.

We now show that G fulfills the 4 properties of a group. Let $a, b, c \in G$.

Associative property: Since a, b, c are all $S \to S$, we get $(a * b) * c = a * (b * c)$ by lemma 1.3.1 in Herstein.

Closed property: We first show $g^n f = f g^{-n}$ by induction. The base case $gf = fg^{-1}$ is done above. For $n > 1$, $g^n f = gfg^{-(n-1)}$. By the associative property, we get

$$g^n f = (gf)g^{-(n-1)} = fg^{-n}. \tag{1}$$

We now show that for $i, j, k, l \in \mathbb{Z}$, $f^i g^j f^k g^l = f^{i+k} g^{(-1)^k j + l}$. If k is even, then $f^i g^j f^k g^l = f^i g^{j+l}$. If k is odd, then $f^i g^j f^k g^l = f^i (g^j f) g^l = f^{i+1} g^{-j+l}$, by (1). Combining two cases, we get a generalized equality

$$f^i g^j f^k g^l = f^{i+k} g^{(-1)^k j + l}. \tag{2}$$

Finally, we show that G is closed under $*$. Let $a = f^i g^j, b = f^k g^l \in G$. Then,

$$\begin{aligned}
(a * b)(x, y) &= (f^i g^j f^k g^l)(x, y) \\
&= (f^{i+k} g^{(-1)^k j + l})(x, y) && \text{by (2)} \\
&= f^{i+k}(g^{(-1)^k j + l \mod 4}(x, y)) \\
&= (f^{i+k \mod 2} g^{(-1)^k j + l \mod 4})(x, y) \in G
\end{aligned}$$

Identity property: Let $a = f^i g^j, e = g^4 = f^2 \in G$. Then, we have

$$\begin{aligned}
a * e &= f^i g^{j+4} = f^i g^j = a, \\
e * a &= f^{i+2} g^j = f^i g^j = a.
\end{aligned}$$

Thus, G has e as the identity element under $*$.

Inverse property: For all $a = f^i g^j \in G$, we have $b = f^i g^{(-1)^i j}$ such that

$$a * b = f^i g^j * f^i g^{(-1)^{i+1} j} = f^{2i} g^{(-1)^i j + (-1)^{i+1} j} = f^0 g^0 = e,$$
$$b * a = f^i g^{(-1)^{i+1} j} * f^i g^j = f^{2i} g^{(-1)^{2i+1} j + j} = f^0 g^0 = e$$

by (2). Thus, the inverse property holds. Since all four properties hold, G is a group under $*$.

We will prove that G is a non-abelian group. Since

$$(f * g)(x, y) = f(g(x, y)) = f(-y, x) = (y, x),$$

but

$$(g * f)(x, y) = g(f(x, y)) = g(-x, y) = (-y, -x),$$

we get that $f * g \neq g * f$. Thus, G is a non-abelian group.

Finally, we prove that G is order of 8. Since there are 2 possible values for i and 4 possible values for j, G has at most 8 elements. We will show that each combination of i, j leads to a distinct $f^i g^j$. Let $a = f^i g^j$, $b = f^k g^l$, for $i, k = 0, 1,\ j, l = 0, 1, 2, 3$, and $i \neq k$ or $j \neq l$. Suppose for the sake of contradiction that $a = b$. Then

$$\begin{aligned} a &= b \\ f^i g^j &= f^k g^l \\ f^{-k} f^i g^j g^{-l} &= e \\ f^{i-k} g^{j-l} &= e. \end{aligned}$$

However, since $i \neq k$ or $j \neq l$, $f^{i-k} g^{j-l} \neq e$, contradiction. Therefore, G has an order of 8. $\square$

Question 2.1.21. Show that a group of order 5 must be abelian.

Proof. Suppose for sake of contradiction that there exists a non-abelian group $G = \{e, f, g, h, j\}$ of order 5 with e as the identity element. Since G is non-abelian, there exists a pair of elements, say f, g, such that $fg \neq gf$, where $fg, gf \in G$. $fg, gf \neq e$ as otherwise it would contradict the rule of inverse. And since $fg, gf \neq f, g$, we know fg, gf must be the rest of the 2 elements, namely h, j. Let $h = fg$ and $j = gf$. Thus, we can represent any non-abelian group of order 5 in the form of $G = \{e, f, g, fg, gf\}$. Note that any non-abelian group of order 5 can be represented in this form. Then,

$$\begin{aligned}
f^2 &\neq f && \text{otherwise } f \neq e \\
f^2 &\neq g && \text{otherwise } fg = fff = gf \\
f^2 &\neq fg, gf && \text{otherwise } f = g \\
fgf &\neq e && \text{otherwise } f(gf) = f(fg) = e \to gf = fg \\
fgf &\neq f, fg, gf && \text{otherwise } e \text{ is not unique}
\end{aligned}$$

Thus, $f^2 = e$ and $fgf = g$. However, $ffg = g = fgf$, and so $fg = gf$, contradiction. Therefore, a group of order 5 must be abelian. □

Question 2.1.23. In the group G of Example 6, find all elements $U \in G$ such that $U * T_{a,b} = T_{a,b} * U$ for every $T_{a,b} \in G$.

Proof. We will show that $U = T_{1,0}$ is the only solution. Let $m, n, a, b, c, d \in \mathbb{R}$. Suppose that $T_{m,n} * T_{a,b} = T_{a,b} * T_{m,n}$, and $T_{m,n} * T_{c,d} = T_{c,d} * T_{m,n}$. Then, for $r \in \mathbb{R}$, we have $mar + mb + n = amr + an + b$ and $mcr + md + n = cmr + cn + d$, and thus we get the system of equations

$$\begin{cases} bm + (1-a)n = b \\ dm + (1-c)n = d. \end{cases}$$

Suppose that $b = 0$, we get $n = 0$ from the first equation. Plugging $n = 0$ into the equation, we get $m = 1$. Suppose that $b \neq 0$, we solve the system and get $(\frac{b-cb-d+da}{b})n = 0$, and thus, in general, $n = 0$. Plugging $n = 0$ into equation 1, we get $m = 1$. Therefore, $U = T_{1,0}$.

$\square$