Abstract Algebra Homework 1

Zachary Meyner

2. Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

Theorem 1. *Let $a, b, c \in G$. Given a is the Identity element of the set G, then $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall b, c \in G$.*

Proof. Let $d \in G$ with $b \circ c = d$. Then $a \circ (b \circ c) \implies a \circ d = d$.
We also have $(a \circ b) \circ c \implies b \circ c = d$.
$\therefore a \circ (b \circ c) = (a \circ b) \circ c$. ■

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

This Cayley Table does not form a group because it is not Associative:

$$\begin{aligned} & a \circ (b \circ c) = d \text{ and} \\ & (a \circ b) \circ c = a \\ \implies & a \circ (b \circ c) \neq (a \circ b) \circ c \end{aligned}$$

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Closure: Every element in the Cayley Table is in the set G, so it is closed.
Identity: taking any element and multiplying it by a returns that element. So a is the indentity element.
Inverse: A diagonal is formed in the table with the identity element a, so every element is its own inverse.
Associative: Because a is the identity element it is associative with every set of two elements by Theorem 1. Because every element $p_{ij} = p_{ji}$ it is commutative as well, so only one permutation of the elements b, c, d needs to be tested for associativity. We have
$(b \circ c) \circ d = a$, and $b \circ (c \circ d) = a$, so $(b \circ c) \circ d = b \circ (c \circ d)$.
Therefore this Cayley Table is a group.

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

This Cayley Table is the same as the Cayley Table for the group $(\mathbb{Z}_4, +)$ where $a = 0,\ b = 1,\ c = 2,\ d = 3$, so This Cayley Table must be a group.

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

The identity element of this Cayley Table is a. There is no inverse for d where $d \circ p = a$ in this Cayley Table. Therefore this Cayley Table is not a Group.

13. Show that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under the operation of multiplication.
Let $a, b, c \in \mathbb{R}^*$
Closure: Multiplying two real numbers will always return result in a real number.
Associativity: The Field Axioms of real numbers state $a * (b * c) = (a * b) * c$, so it is Associative as well.
Identity: The multiplicative identity for $\mathbb{R}^*$ is 1 because $a \cdot 1 = a\ \forall a \in \mathbb{R}^*$.
Inverse: The multiplicative inverse for $\mathbb{R}^*$ is $\frac{1}{a}$ because $a \cdot \frac{1}{a} = \frac{a \cdot 1}{a} = \frac{a}{a} = 1\ \forall a \in \mathbb{R}^*$.

27. Prove that the inverse of $g_1g_2\dots g_n$ is $g_n^{-1}g_{n-1}^{-1}\dots g_1^{-1}$.

Proof by induction. Base Case ($n=1$):

$$g_1g_1^{-1} = g_1^{-1}g_1 = e$$

Inductive Hypothesis ($n=k$):

$$(g_1g_2\dots g_k)(g_k^{-1}g_{k-1}^{-1}\dots g_1^{-1}) = (g_k^{-1}g_{k-1}^{-1}\dots g_1^{-1})(g_1g_2\dots g_k) = e$$

Inductive Step ($n=k+1$)
(WTS: $(g_1g_2\dots g_{k+1})(g_{k+1}^{-1}g_k^{-1}\dots g_1^{-1}) = (g_{k+1}^{-1}g_k^{-1}\dots g_1^{-1})(g_1g_2\dots g_{k+1}) = e$)

$$\begin{aligned}
&(g_1g_2\dots g_{k+1})(g_{k+1}^{-1}g_k^{-1}\dots g_1^{-1}) & \\
&= (g_1g_2\dots g_k)(g_{k+1})(g_{k+1}^{-1})(g_k^{-1}g_{k-1}^{-1}\dots g_1^{-1}) & \text{(Associative Property)}\\
&= (g_1g_2\dots g_k)(e)(g_k^{-1}g_{k-1}^{-1}\dots g_1^{-1}) & \text{(Definition)}\\
&= (g_1g_2\dots g_k)(g_k^{-1}g_{k-1}^{-1}\dots g_1^{-1}) & \text{(Definition)}\\
&= e & \text{(Inductive Hypothesis)}
\end{aligned}$$

and

$$\begin{aligned}
&(g_{k+1}^{-1}g_k^{-1}\dots g_1^{-1})(g_1g_2\dots g_{k+1}) & \\
&= g_{k+1}^{-1}(g_k^{-1}g_{k-1}^{-1}\dots g_2g_1^{-1})(g_1g_2g_3\dots g_k)g_{k+1} & \text{(Associative Property)}\\
&= (g_{k+1}^{-1})(e)(g_{k+1}) & \text{(Inductive Hypothesis)}\\
&= (g_{k+1}^{-1})(g_{k+1}) & \text{(Definition)}\\
&= e & \text{(Definition)}
\end{aligned}$$

$\therefore (g_1g_2\dots g_n)(g_n^{-1}g_n^{-1}\dots g_1^{-1}) = (g_n^{-1}g_{n-1}^{-1}\dots g_1^{-1})(g_1g_2\dots g_n) = e$ ■

31. Show that if $a^2 = e$ for all elements in a in a group G, then G must be abelian.

Proof. Let $a, b \in G$. Consider $a\cdot b\cdot b\cdot a$. Since $a^2 = a\cdot a = e\ \forall a \in G$, and G is a Group, we have

$$\begin{aligned}
a\cdot b\cdot b\cdot a &= a\cdot(b\cdot b)\cdot a & \text{(Commutative Property)}\\
&= a\cdot e\cdot a & \text{(Hypothesis)}\\
&= a\cdot a & \text{(Identity Property)}\\
&= e & \text{(Hypothesis)}
\end{aligned}$$

But $a\cdot b$ has an inverse element of $a\cdot b$, and we have proven that $(a\cdot b)\cdot(b\cdot a) = e$, so $a\cdot b = b\cdot a\ \forall a, b \in G$. Therefore G is commutative which makes it an Abelian Group. ■