Math 335, Homework 2

Due Wednesday, February 10

Mark S Kim

---

1. Define a binary operation $*$ on $\mathbb{Z}$ by
$$a * b = 2a + 2b.$$
So, for example,
$$1 * 3 = 2 \cdot 1 + 2 \cdot 3 = 8.$$
Use a specific example to show that $*$ is *not* associative.

   Answer:
   Let $a = 0, b = 0, c = 1$. Then
$$\begin{aligned}(a * b) * c &= (2a + 2b) * c = 2(2a + 2b) + 2c \\ &= 2(2 \cdot 0 + 2 \cdot 0) + 2(1) = 2 \\ a * (b * c) &= a * (2b + 2c) = 2a + 2(2b + 2c) \\ &= 2 \cdot 0 + 2(2 \cdot 0 + 2 \cdot 1) = 4.\end{aligned}$$
   Hence, $(a * b) * c \neq a * (b * c)$ and $*$ is not associative.

2. Let
$$G = \{5, 15, 25, 35\}.$$
Prove that G is a group under the operation of multiplication modulo 40. You can assume that multiplication is associative, but you should prove closure, the existence of an identity, and the existence of inverses. (**Hint**: Make a multiplication table.)

   Answer:

$\times$	5	15	25	35
5	$25 \equiv 25 \mod 40$	$75 \equiv 35 \mod 40$	$125 \equiv 5 \mod 40$	$175 \equiv 15 \mod 40$
15	$75 \equiv 35 \mod 40$	$225 \equiv 25 \mod 40$	$375 \equiv 15 \mod 40$	$525 \equiv 5 \mod 40$
25	$125 \equiv 5 \mod 40$	$375 \equiv 15 \mod 40$	$625 \equiv 25 \mod 40$	$875 \equiv 35 \mod 40$
35	$175 \equiv 15 \mod 40$	$525 \equiv 5 \mod 40$	$875 \equiv 35 \mod 40$	$1225 \equiv 25 \mod 40$

   0. Closure: ✓: notice from the table above that G is closed under the operation of multiplication modulo 40.
   1. Associativity: ✓: assumed.
   2. Identity: ✓: $e = 25 \in G$. Notice that
$$\begin{aligned}5 \cdot 25 = 125 &\equiv 5 \mod 40 \\ 15 \cdot 25 = 375 &\equiv 15 \mod 40 \\ 25 \cdot 25 = 625 &\equiv 25 \mod 40 \\ 35 \cdot 25 = 875 &\equiv 35 \mod 40\end{aligned}$$

3. Inverse: $\checkmark$: notice from the table that the inverse of a is a. So $a \cdot a = e$ for all $a \in G$.

$$\begin{aligned} 5 \cdot 5 &= 25 \equiv 25 \mod 40 \\ 15 \cdot 15 &= 225 \equiv 25 \mod 40 \\ 25 \cdot 25 &= 625 \equiv 25 \mod 40 \\ 35 \cdot 35 &= 1225 \equiv 25 \mod 40 \end{aligned}$$

3. Let n be any positive integer, and let

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

(This is called the set of n**th roots of unity**.) For example,

$$\begin{aligned} U_2 &= \{1, -1\} \\ U_4 &= \{1, -1, i, -i\}, \end{aligned}$$

or, more weirdly,

$$U_3 = \left\{1,\ -\frac{1}{2} + \frac{\sqrt{3}}{2}i,\ -\frac{1}{2} - \frac{\sqrt{3}}{2}i\right\}.$$

(Don't worry, I'd never expect you to know that last one on your own!) Prove that, for all n, the set U_n is a group under the operation of multiplication. You can assume that multiplication is associative, but you should prove closure, the existence of an identity, and the existence of inverses.

Answer:

0. Closure: $\checkmark$
   Consider x^n, $y^n \in U_n$. To prove closure, we must show that $(x \cdot y) \in U_n$. Since $x^n = 1$, $y^n = 1$, and $1 \cdot 1 = 1$, $x^n \cdot y^n = 1$. Then

$$\begin{aligned} 1 &= x^n \cdot y^n \\ &= (x \cdot y)^n. \end{aligned}$$

   Hence, U_n is closed under the operation of multiplication.
1. Associativity: $\checkmark$: assumed.
2. Identity: $\checkmark$: Since $z^n \cdot 1 = 1 \cdot x^n = z^n$ for all $z^n \in U_n$, the identity for U_n exists and equals 1.
3. Inverse: $\checkmark$
   Suppose the inverse to $z^n \in U_n$ is w^n. We need to prove that $w^n \in U_n$. By definition, $z^n \cdot w^n = e = 1$, so $w^n = \frac{1}{z^n}$. Since $w^n = \frac{1}{z^n} = \frac{1}{1} = 1 \in U_n$, w^n exists and is in U_n.

4. Find an example of three elements $a, b, c \in D_4$ such that

$$b \circ a = a \circ c \quad \text{but} \quad b \neq c.$$

What does this tell you about the cancellation property in D_4?

Answer:
For $a, b, c \in D_4$, an example that satisfies the given property is $a = R_{90}$, $b = H$, and $c = V$, so $H \circ R_{90} = R_{90} \circ V = D$.

The left cancellation property states that $a * b = a * c \implies b = c$, and the right cancellation property states that $b * a = c * a \implies b = c$. The above statement implies that the cancellation property in D_4 is *not* commutative (but may be commutative in certain cases).

In Problems 5, we use exponents to indicate doing the group operation repeatedly. That is, let G be a group with operation $*$ and let $a \in G$. Then we write a^2 to mean $a * a$, we write a^3 to mean $a * a * a$, and so on.

5. Let G be any group and let $a, b \in G$. Prove that $(a*b)^2 = a^2*b^2$ if and only if $a*b = b*a$.

Proof. For the forward direction, let $(a * b)^2 = a^2 * b^2$. Then

$$\begin{aligned}
(a * b)^2 &= a^2 * b^2 \\
(a * b) * (a * b) &= (a * a) * (b * b) \\
a * (b * a) * b &= a * (a * b) * b \quad \text{by associativity} \\
b * a &= a * b \quad \text{using cancellation property}
\end{aligned}$$

For the reverse direction, let $a * b = b * a$. Then

$$\begin{aligned}
(a * b)^2 &= (a * b) * (a * b) \\
&= a * (b * a) * b \quad \text{by associativity} \\
&= a * (a * b) * a \quad \text{given} \\
&= (a * a) * (b * b) \quad \text{by associativity} \\
&= a^2 * b^2
\end{aligned}$$

$\square$