Remember:

When checking whether a set G, and an operation $*$ is a group, check whether

1. *G is closed under the operation:* Let $a, b \in G$. Is $a * b \in G$?
2. *$*$ is associative:* Let $a, b, c \in G$. Does $a * (b * c) = (a * b) * c$?
3. *G has an identity:* Is there an element $e \in G \ni$ for all $a \in G$, $e * a = a = a * e$?
4. *every element in G has an inverse:* Let $a \in G$. Is there an element $b \in G$ such that $a * b = e = b * a$?

In Class Work

1. For all $n > 1$, define $U(n)$ to be the set $\{a \in \mathbb{Z}^+ | a < n \text{ and } \gcd(n, a) = 1\}$.
   (a) What are the elements of $U(12)$?
   (b) Write out the Cayley table for $U(12)$.
   (c) Show that $U(12)$ is a group under multiplication mod 12.
2. $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$ are groups under addition mod 2 and mod 3 respectively. Define $Z_2 \oplus \mathbb{Z}_3$ to be the set $\{(a, b) | a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$. Define the operation on $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ to be component-wise addition. That is, if $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$, define $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2 \text{ mod } 2, b_1 + b_2 \text{ mod } 3)$. Show that $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is a group under this operation.

Solutions

1. For all $n > 1$, define $U(n)$ to be the set $\{a \in \mathbb{Z}^+ | a < n \text{ and } \gcd(n, a) = 1\}$.
   (a) What are the elements of $U(12)$?

   $U(12) = \{1, 5, 7, 11\}$, as these are the only integers positive integers less than 12 which have no divisors in common with 12 other than 1.

   (b) Write out the Cayley table for $U(12)$:

Cayley Table for U(12)

$\cdot$ mod 12	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

1(c) Is $U(12)$ a group under multiplication (mod 12)?

0.1 Closed under multiplication mod 12?

We can see by looking at the Cayley table that for any $a, b \in U(12), ab \in U(12)$.

0.2 Associative?

Since multiplication in the integers is associative, and since multiplication mod 12 is simply the remainder after doing regular integer multiplication, multiplication mod 12 is also associative.

0.3 Identity?

Multiplying by 1 mod 12 leaves every number unchanged, and so 1 is the identity.

0.4 Closed under inverses?

By looking at the Cayley table, I can see that each number has a unique inverse:

$$(1)^{-1} = 1 \qquad (5)^{-1} = 5 \qquad 7^{-1} = 7 \qquad 11^{-1} = 11$$

Notice: each number is its own inverse!

2. Show that $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is a group under componentwise addition.

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0),(1,0),(0,1),(1,1),(0,2),(1,2)\}$
- **Closed under the operation?**

  Let $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$.
  NTS $(a_1, b_1) + (a_2, b_2) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2 \bmod 2, b_1 + b_2 \bmod 3).$$

  $a_1 + a_2 \bmod 2 \in \mathbb{Z}_2,\ b_1 + b_2 \bmod 3 \in \mathbb{Z}_3$
  $\implies (a_1, b_1) + (a_2, b_2) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$
  $\implies G$ is closed under component-wise addition.

2. (continued)

- **Associative?**

  This follows simply from addition of integers being associative, but let's see why:

  Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$.

$$\begin{aligned}
&\Big[(a_1, b_1) + (a_2, b_2)\Big] + (a_3, b_3) \\
&\qquad = (a_1 + a_2 \bmod 2, b_1 + b_2 \bmod 3) + (a_3, b_3) \\
&\qquad = \Big((a_1 + a_2) + a_3 \bmod 2, (b_1 + b_2) + b_3 \bmod 3\Big) \\
&\qquad = \Big(a_1 + (a_2 + a_3) \bmod 2, b_1 + (b_2 + b_3) \bmod 3\Big) \\
&\qquad = (a_1, b_1) + (a_2 + a_3, b_2 + b_3) \\
&\qquad = (a_1, b_1) + \Big[(a_2, b_2) + (a_3, b_3)\Big]
\end{aligned}$$

  Therefore the operation *is* associative.

2. (continued)

- **Identity**?
  $(0, 0) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$.
  For all $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$,
  $(0, 0) + (a, b) = (0 + a \bmod 2, 0 + b \bmod 3) = (a, b)$ and vice versa.
- **Closed under inverses**?
  Since $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are groups, for all $a \in \mathbb{Z}_2$, there exists an additive inverse $-a$, and for all $b \in \mathbb{Z}_3$, there also exists an additive inverse $-b$.
  For example, in $\mathbb{Z}_2$, $-1 = 1$ and in $\mathbb{Z}_3$, $-1 = 2$. Thus for all $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_3$, there exists $(-a, -b)$, and
  $(a, b) + (-a, -b) = (a - a \bmod 2, b - b \bmod 3) = (0, 0)$.

Thus $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is a group under componentwise addition.

Notation:

What we're trying to denote	If the operation is addition	anything but addition
the inverse of g	$-g$	g^{-1}
$g * g$ n times	ng	g^n
the identity	$0 = e$	$1 = e$

Important: This is *just* notation!

In Class Work

3. Define the set $\mathbb{Z}[\sqrt{2}]$ as follows:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}.$$

Show that $\mathbb{Z}[\sqrt{2}]$ is an Abelian group under addition.

Solutions:

3. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$. Show $\mathbb{Z}[\sqrt{2}]$ is an Abelian group under addition.

   - **Closed under the operation?**
     Let $a_1 + b_1\sqrt{2}$, $a_2 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
     NTS $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$.

     $$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}.$$

     Since $a_1 + a_2$, $b_1 + b_2 \in \mathbb{Z}$, the sum *is* in $\mathbb{Z}[\sqrt{2}]$, and so the set is closed under the operation.

   - **Associative?**
     This set is just a subset of the reals, and addition in the reals is of course associative.

3. (continued)

- **Identity?**
  $0 = 0 + 0\sqrt{2}$ is of course in $\mathbb{Z}[\sqrt{2}]$, and 0 carries its additive identity property over from the reals.
- **Closed under inverses?**
  Let $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then $-a - b\sqrt{2}$ is also in $\mathbb{Z}[\sqrt{2}]$, and $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0$.
  Thus every element in $\mathbb{Z}[\sqrt{2}]$ has an additive inverse that is again in $\mathbb{Z}[\sqrt{2}]$, and so it is closed under inverses.

Thus $\mathbb{Z}[\sqrt{2}]$ is a group under addition.