In Class Work

1. Is $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ a group under multiplication mod 6?

Definition:

Let G be a non-empty set with a binary operation. If a and b are both elements of G, denote the result of the operation on the pair (a, b) by ab.

Note: when we don't know what the elements of G are, and we don't know the operation, we use multiplication notation, as above. If we **do** *know the operation, then we would of course use whatever the appropriate notation would be.*

Definition:

Let G be a non-empty set with a binary operation. If a and b are both elements of G, denote the result of the operation on the pair (a, b) by ab.

Note: when we don't know what the elements of G are, and we don't know the operation, we use multiplication notation, as above. If we **do** *know the operation, then we would of course use whatever the appropriate notation would be.*

Then we say that G is a **group** under the operation if the following are satisfied:

Definition:

Let G be a non-empty set with a binary operation. If a and b are both elements of G, denote the result of the operation on the pair (a, b) by ab.

Note: when we don't know what the elements of G are, and we don't know the operation, we use multiplication notation, as above. If we **do** *know the operation, then we would of course use whatever the appropriate notation would be.*

Then we say that G is a **group** under the operation if the following are satisfied:

1. *Associativity:* $(ab)c = a(bc)$ for all $a, b, c \in G$.

Definition:

Let G be a non-empty set with a binary operation. If a and b are both elements of G, denote the result of the operation on the pair (a, b) by ab.

Note: when we don't know what the elements of G are, and we don't know the operation, we use multiplication notation, as above. If we **do** *know the operation, then we would of course use whatever the appropriate notation would be.*

Then we say that G is a **group** under the operation if the following are satisfied:

1. *Associativity:* $(ab)c = a(bc)$ for all $a, b, c \in G$.
2. *Identity:* There exists $e \in G$ such that $ae = ea = a$ for all $a \in G$.

Definition:

Let G be a non-empty set with a binary operation. If a and b are both elements of G, denote the result of the operation on the pair (a, b) by ab.

Note: when we don't know what the elements of G are, and we don't know the operation, we use multiplication notation, as above. If we **do** *know the operation, then we would of course use whatever the appropriate notation would be.*

Then we say that G is a **group** under the operation if the following are satisfied:

1. *Associativity:* $(ab)c = a(bc)$ for all $a, b, c \in G$.
2. *Identity:* There exists $e \in G$ such that $ae = ea = a$ for all $a \in G$.
3. *Inverse:* For every $a \in G$, there exists $b \in G$ such that $ab = ba = e$.

More Definitions:

- Let G be a set. An operation $*$ is a **binary operation on** G if for all $g, h \in G$, $g * h \in G$.
- G is **closed** under the operation $*$, if $*$ is binary; that is, if for all $g, h \in G$, $g * h \in G$.

When checking whether G is a group, check

- *Closed under the operation*–for all $a, b \in G$, ab must also be in G.
- *Associative*
- *Identity*
- *Inverses*

Cayley Table for $\mathbb{Z}_6$ under multiplication mod 6:

$\times$ mod 6	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

More In Class Work

1. Is $S = \{f : \mathbb{R} \to \mathbb{R} | f \text{ is one-to-one and onto}\}$ a group under composition?

- **Is S closed under the operation?**
  Showed this earlier!
- **Is $\circ$ associative?**
  Let $f, g, h \in S$. Is $f \circ (g \circ h) = (f \circ g) \circ h$?
  We know that composition is associative.
- **Is there an element which acts as an identity in S?**
  In other words, is there a function e in S so that $f \circ e = f = e \circ f$?
  Consider the *identity* function $e : \mathbb{R} \to \mathbb{R}$ so that $e(x) = x$. e is clearly in S (just check each of the requirements in the definition of S), and equally clearly, $f \circ e = f = e \circ f$. Thus there *is* an identity element in S.
- For all $f \in S$, does there exist $g \in S$ such that $f \circ g = e$?
  Since f is 1-1 and onto, there exists an inverse function f^{-1} such that $f \circ f^{-1} = e = f^{-1} \circ f$. But is f^{-1} in S?
  $f^{-1} : \mathbb{R} \to \mathbb{R}$, and is also 1-1 and onto (check!), so f^{-1} must be in S also. Thus every element in S has an inverse element in S.

Therefore S is a group.