

**Activity 18.11**

(a) In a group  $G$  with identity  $e$ , if  $ab = e$  for some  $a, b \in G$  must it follow that  $b = a^{-1}$ ?

**Conjecture.** In a group  $G$  with identity  $e$ , if  $ab = e$  for some  $a, b \in G$ , then  $ba = e$  and consequently  $b = a^{-1}$ .

*Proof.* Let  $G$  be a group with identity  $e$  and let  $a, b \in G$  such that

$$ab = e. \quad (1)$$

Multiplying  $a$  on the right side of (1) we obtain

$$(ab)a = ea. \quad (2)$$

Applying the associative property of groups from (2) we know that

$$a(ba) = ea. \quad (3)$$

Because  $e$  is the identity of  $G$ ,

$$ea = ae. \quad (4)$$

Applying the transitive property of equality to (3) and (4) we obtain

$$a(ba) = ae. \quad (5)$$

Applying the group cancellation law to (5) we obtain

$$ba = e. \quad (6)$$

In conclusion we have shown that in a group  $G$  with identity  $e$ , if  $ab = e$  for some  $a, b \in G$ , then  $ba = e$ . From the fact that  $ab = e$  and  $ba = e$  we can conclude that  $b$  is the inverse of  $a$ .  $\square$

(a) In a group  $G$  with identity  $e$ , if  $ba = e$  for some  $a, b \in G$  must it follow that  $b = a^{-1}$ ?

**Conjecture.** In a group  $G$  with identity  $e$ , if  $ba = e$  for some  $a, b \in G$ , then  $ab = e$  and consequently  $b = a^{-1}$ .

*Proof.* Let  $G$  be a group with identity  $e$  and let  $a, b \in G$  such that

$$ba = e. \quad (7)$$

Multiplying  $a$  on the left side of (7) we obtain

$$a(ba) = ae. \quad (8)$$

Applying the associative property of groups from (8) we know that

$$(ab)a = ae. \quad (9)$$

Because  $e$  is the identity of  $G$ ,

$$ae = ea. \quad (10)$$

Applying the transitive property of equality to (9) and (10) we obtain

$$(ab)a = ea. \quad (11)$$

Applying the group cancellation law to (11) we obtain

$$ab = e. \quad (12)$$

In conclusion we have shown that in a group  $G$  with identity  $e$ , if  $ba = e$  for some  $a, b \in G$ , then  $ab = e$ . From the fact that  $ab = e$  and  $ba = e$  we can conclude that  $b$  is the inverse of  $a$ .  $\square$

(c) Let  $f$  and  $g$  be functions from a set  $S$  to  $S$ . Let  $I$  be the identity function on  $S$  – that is  $I(x) = x$  for all  $x$  in  $S$ . Show by example that it is possible to have  $fg = I$ , but  $f \neq g^{-1}$ . Does this violate part (a)? Explain.

Let  $f$  and  $g$  be functions from the set  $\mathbb{C}$  to  $\mathbb{C}$  defined as  $f(x) = x^2$  and  $g(x) = \sqrt{x}$ . Now  $f \circ g(x) = x$ , however  $g \circ f(x) = |x|$  and so  $f$  is not the inverse of  $g$ . This fact does not violate what we found in part (a), because this statement applies only to groups and  $g$  is not a group.

(4) Determine if the set  $G$  is a group under the indicated operation. If  $G$  is a group, verify that each group property is satisfied. If  $G$  is not a group, provide examples that show which of the group properties are not satisfied.

(a) Let  $G$  be the set of odd integers under addition.

The set  $G$  is not a group. The identity element for this set must be zero, but zero is not an odd integer. Therefore,  $G$  does not have an identity element and is not a group.

(b) Let  $G = [2], [4], [6], [8] \subset \mathbb{Z}_{10}$ , with the operation of multiplication of congruence classes.

First we will construct an operation table for this group.

$\cdot$	$[2]$	$[4]$	$[6]$	$[8]$
$[2]$	$[4]$	$[8]$	$[2]$	$[6]$
$[4]$	$[8]$	$[6]$	$[4]$	$[2]$
$[6]$	$[2]$	$[4]$	$[6]$	$[8]$
$[8]$	$[6]$	$[2]$	$[8]$	$[4]$

From this operation table we see that  $a \cdot [6] = [6] \cdot a = a$  for all  $a \in G$  and so  $[6]$  is  $G$ 's identity element. We can also see from the operation table that for all  $a \in G$  there exists a  $b \in G$  such that  $a \cdot b = b \cdot a = [6]$  and so every element has an inverse. There are no elements in the operation table that are not in  $G$  and so  $G$  is closed under multiplication of congruence classes. We already know that multiplication of congruence classes is associative and so it will be associative in  $G$ .

In conclusion, we have shown that the set  $G$  has an identity, is closed, is associative, and each element has an inverse under multiplication of congruence classes. Therefore,  $G$  is a group under multiplication of congruence classes.

(c) Let  $G = [0], [2], [4], [6], [8] \subset \mathbb{Z}_{10}$ , with the operation of addition of congruence classes.

First we will construct an operation table for this group.

+	[0]	[2]	[4]	[6]	[8]
[0]	[0]	[2]	[4]	[6]	[8]
[2]	[2]	[4]	[6]	[8]	[0]
[4]	[4]	[6]	[8]	[0]	[2]
[6]	[6]	[8]	[0]	[2]	[4]
[8]	[8]	[0]	[2]	[4]	[6]

From this operation table we see that  $a + [0] = [0] + a = a$  for all  $a \in G$  and so  $[0]$  is  $G$ 's identity element. We can also see from the operation table that for all  $a \in G$  there exists a  $b \in G$  such that  $a + b = b + a = [0]$  and so every element has an inverse. There are no elements in the operation table that are not in  $G$  and so  $G$  is closed under addition of congruence classes. We already know that addition of congruence classes is associative and so it will be associative in  $G$ .

In conclusion, we have shown that the set  $G$  has an identity, is closed, is associative, and each element has an inverse under addition of congruence classes. Therefore,  $G$  is a group under addition of congruence classes.

(d) Let  $G = q \in \mathbb{Q} : q \neq 1$ , with the operation  $*$  defined by  $a * b = a + b - ab$ .

First we note that  $a * 0 = 0 * a = a$  for all  $a \in G$  and so  $0$  is the identity element in  $G$ . We know that integers are associative under addition and this operation can be defined using only addition. Therefore  $G$  is associative under the operator  $*$ . Next we will show that  $G$  is closed.

*Proof.* Let  $a, b \in G$  such that

$$a + b - ab = 1 \quad (13)$$

We are working with integers under addition and subtraction which we now is commutative and associative. We subtract  $b$  from (13) to obtain

$$a - ab = 1 - b. \quad (14)$$

Factoring out  $a$  on the left side of (14) we obtain

$$a(1 - b) = 1 - b \quad (15)$$

From (14) we can apply the group cancellation law to arrive at the contradiction

$$a = 1.$$

From this contradiction, we know that  $G$  is closed under the operation  $*$ .  $\square$

Finally we will show that every element has an inverse. Let  $a, b \in G$  such that

$$b = \frac{a}{a - 1}.$$

The element  $b$  is only undefined when  $a = 1$  and there is no  $a$  such that  $b = 1$ . We can also see that

$$a + b - ab = b + a - ba = a + \frac{a}{a - 1} - \frac{a \cdot a}{a - 1} = 0.$$

From this we see that each element  $a \in G$  has an inverse and this inverse is  $\frac{a}{a - 1}$ .

In conclusion, we have shown that the set  $G$  has an identity, is closed, is associative, and each element has an inverse under the operator  $*$ . Therefore,  $G$  is a group under the operator  $*$ .

(e) Let  $G = [x] \in \mathbb{Z}_9 : x = 1, 2, 4, 5, 7, \text{ or } 8$ , with the operation  $[x] * [y] = [x][y]$ .

First we will construct an operation table.

$*$	[1]	[2]	[4]	[5]	[7]	[8]
[1]	[1]	[2]	[4]	[5]	[7]	[8]
[2]	[2]	[4]	[8]	[1]	[5]	[7]
[4]	[4]	[8]	[7]	[2]	[1]	[5]
[5]	[5]	[1]	[2]	[7]	[8]	[4]
[7]	[7]	[5]	[1]	[8]	[4]	[2]
[8]	[8]	[7]	[5]	[4]	[2]	[1]

From this operation table we see that  $a * [1] = [1] * a = a$  for all  $a \in G$  and so  $[1]$  is  $G$ 's identity element. We can also see from the operation table that for all  $a \in G$  there exists a  $b \in G$  such that  $a * b = b * a = [1]$  and so every element has an inverse. There are no elements in the operation table that are not in  $G$  and so  $G$  is closed under the binary operator  $*$ . We already know that multiplication of congruence classes is associative and so it will be associative in  $G$ .

In conclusion, we have shown that the set  $G$  has an identity, is closed, is associative, and each element has an inverse under the operator  $*$ . Therefore,  $G$  is a group under the operator  $*$ .