Russ Johnson
Problem Set #2
January 29, 2013

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

$$ab = e. \tag{1}$$

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

$$(ab)a = ea. \tag{2}$$

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

$$a(ba) = ea. \tag{3}$$

Because e is the identity of G we can commute e in (3) to obtain

$$a(ba) = ae. \tag{4}$$

Applying the group cancellation law to (4) we obtain

$$ba = e. \tag{5}$$

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. □

(b) 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

$$ba = e. \tag{6}$$

Multiplying a on the left side of (6) we obtain

$$a(ba) = ae. \tag{7}$$

Applying the associative property of groups from (7) we know that

$$(ab)a = ae. \tag{8}$$

Because e is the identity of G we can commute e in (8) to obtain

$$(ab)a = ea. \tag{9}$$

Applying the group cancellation law to (9) we obtain

$$ab = e. \tag{10}$$

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 f is not in a group. For the function f, $f(2) = f(-2) = 4$ and so it cannot have an inverse, because a function would only be able to map 4 to 2 or to -2 and not both. From this we see that f is not in a group and so what we found in parts (a) and (b) does not apply here.

(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 because it is a subset of the integers, 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 exits some $b \in G$ such that $a \cdot b = b \cdot a = [6]$ and so every element in G 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 in the set $\mathbb{Z}_{10}$ and so it will be associative in its subset 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 exits some $b \in G$ such that $a + b = b + a = [0]$ and so every element in G 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 in the set $\mathbb{Z}_{10}$ and so it will be associative in its subset 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 $G = q \in Q : q \neq 1$, with the operation $*$ defined by $a * b = a + b - ab$.

Let $a \in G$. First we note that $a*0 = a+0-a\cdot 0 = a$ and $0*a = 0+a-0\cdot a = a$ for all $a \in G$ and so 0 is the identity element in G. Let $b \in G$. We know that rational numbers are associative under addition, subtraction, and multiplication and so the operator $*$ will be associative in the set $\mathbb{Q}$. Therefore, $G \subset \mathbb{Q}$ is associative under the operator $*$. Next we will show that G is closed under $*$.

Proof. We will prove that G is closed under $*$ by contradiction. Assume there exist some a and b in G such that

$$a + b - ab = 1 \tag{11}$$

We are working with rational numbers under addition, subtraction, and multiplication and so we can apply some simple algebra. We add the inverse of b in (11) to obtain

$$a - ab = 1 + -b. \tag{12}$$

Applying the distributive property of multiplication over subtraction to (12) we obtain

$$a(1-b) = 1 - b \tag{13}$$

From (12) 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 operator $*$. $\square$

Finally we will show that every element has an inverse. Let $a \in G$. The inverse of a is $b \in G$ 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 every element in G has an inverse.

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 exits some $b \in G$ 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 in $\mathbb{Z}_9$ and so it will be associative in its subset 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 $*$.

(7) Let k be an integer, and let $Z(k)$ be the set of integers on which an operation $\oplus_k$ is defined as follows: $a \oplus_k b = a + b - k$, where $a + b$ denotes the standard sum of a and b in $\mathbb{Z}$. Note that the set $Z(0)$ is the group of integers under the standard addition. For which values of k is $Z(k)$ a group under the operation $\oplus_k$?

Conjecture. The set $Z(k)$ is a group for all $k \in \mathbb{Z}$.

First of all we note that $a + k - k = k + a - k = a$, and so k is the identity element. This is consistent with the fact that 0 is the identity element of integers under addition, $Z(0)$. Next we note that the operation $\oplus$ can be defined using only addition as $a \oplus_k b = a + b + -k$. We already know that the set of integers is associative under addition and so the set of integers is associate under $\oplus_k$ for all $k \in \mathbb{Z}$. The set of integers are closed under addition and subtraction and so $\mathbb{Z}$ is closed under $\oplus_k$, because it consists of only addition and subtraction. Finally, every element $a \in Z(k)$ has an inverse. We see that $a + -a - k = -a + a - k = k$ and so the inverse of the arbitrary element $a \in Z(k)$ is $-a$.

In conclusion, we have shown that $Z(k)$ has an identity element, is associative, is closed, and each element has an inverse for all $k \in \mathbb{Z}$. Therefore $Z(k)$ is a group for all $k \in \mathbb{Z}$.

(8) Prove that a group G is Abelian if and only if $(ab)^2 = a^2b^2$ for all

$a, b \in G$.

Proof. First we will show that if a group G is Abelian, then $(ab)^2 = a^2b^2$ for all $a, b \in G$.

Let G be an abelian group and let $a, b \in G$. First of all,

$$(ab)^2 = (ab)(ab). \tag{14}$$

First, we apply the associative property of the group G to to obtain

$$(ab)^2 = a(ba)b. \tag{15}$$

Next, we use the commutative property of G on (15) to obtain

$$(ab)^2 = a(ab)b. \tag{16}$$

Finally, applying the associative property to (16) we obtain

$$(ab)^2 = a^2b^2.$$

Next we will show that if $(ab)^2 = a^2b^2$ for all $a, b \in G$, then G is Abelian. Let G be a group such that

$$(ab)^2 = a^2b^2 \tag{17}$$

for all $a, b \in G$. From (17) we also know that

$$(ab)(ab) = (aa)(bb). \tag{18}$$

Applying the associative property to (18) we obtain

$$a((ba)b) = a((ab)b). \tag{19}$$

Applying the group cancellation law to (19) we know that

$$(ba)b = (ab)b. \tag{20}$$

Applying the group cancellation law to (20) we obtain

$$ba = ab.$$

From this we can conclude that G is Abelian.

In conclusion, we have shown that if a group G is Abelian, then $(ab)^2 = a^2b^2$ for all $a, b \in G$. We have also shown that if $(ab)^2 = a^2b^2$ for all $a, b \in G$, then G is Abelian. Therefore we have shown that a group G is Abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$. $\square$

(1) Let G be a group.
(a) Let $a, b, c \in G$. What element is $(abc)^{-1}$?

Conjecture. The inverse of abc is $c^{-1}b^{-1}a^{-1}$.

Proof. Let G be a group and let $a, b, c \in G$. First of all, we know that

$$(abc)(c^{-1}b^{-1}a^{-1}) = (abc)(c^{-1}b^{-1}a^{-1}) \tag{21}$$

from the reflexive property of equality. Applying the associative property to (21) we obtain

$$(abc)(c^{-1}b^{-1}a^{-1}) = (ab(cc^{-1})(b^{-1}a^{-1}). \tag{22}$$

Multiplying c and the inverse of c in (22) we obtain the identity element of G, e.

$$(abc)(c^{-1}b^{-1}a^{-1}) = (abe)(b^{-1}a^{-1}). \tag{23}$$

The identity element can be multiplied out of (23) to obtain

$$(abc)(c^{-1}b^{-1}a^{-1}) = (ab)(b^{-1}a^{-1}). \tag{24}$$

Repeating this process we see that

$$(abc)(c^{-1}b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

We can also apply the same rules to show that

$$(c^{-1}b^{-1}a^{-1})(abc) = (c^{-1}b^{-1})(bc) = c^{-1}c = e.$$

In conclusion, we have shown that

$$(c^{-1}b^{-1}a^{-1})(abc) = (abc)(c^{-1}b^{-1}a^{-1} = e$$

and therefore the inverse of abc is $c^{-1}b^{-1}a^{-1}$. $\square$

(b) Let m be a positive integer, and let $a_1, a_2, \ldots, a_m$ be elements in G. What element is $(a_1a_2 \cdots a_m)^{-1}$?

Conjecture. The inverse of $a_1a_2 \ldots a_m$ is $a_m^{-1}a_{m-1}^{-1} \ldots a_1^{-1}$ for all $m \in \mathbb{Z}^+$.

Proof. We will prove our conjecture using induction. First we note that for $m = 1$ we have $a_1^{-1} = a_1^{-1}$ and for $m = 2$ we have $(a_1a_2)^{-1} = a_2^{-1}a_1^{-1}$. The equation for $m = 1$ is self-evident. For $m = 2$ we see that

$$(a_1a_2)(a_2^{-1}a_1^{-1}) = a_1(a_2a_2^{-1})a_1^{-1} = a_1ea_1^{-1} = a_1a_1^{-1} = e$$

and

$$(a_2^{-1}a_1^{-1})(a_1a_2) = a_2^{-1}(a_1^{-1}a_1)a_2 = a_2^{-1}ea_2 = a_2^{-1}a_2 = e.$$

And so, for $m = 2$ the conjecture is true.
For the next part of the proof we will show that

$$(a_1a_2\dots a_m)^{-1} = a_m^{-1}a_{m-1}^{-1}\dots a_1^{-1}$$

implies that

$$(a_1a_2\dots a_ma_{m+1})(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1}) = e$$

and

$$(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1})(a_1a_2\dots a_ma_{m+1}) = e$$

and therefore the inverse of $a_1a_2\dots a_ma_{m+1}$ is $a_{m+1}^{-}1a_m^{-1}a_{m-1}^{-1}\dots a_1^{-1}$. First of all,

$$(a_1a_2\dots a_ma_{m+1})(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1}) = (a_1a_2\dots a_ma_{m+1})(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1}). \tag{25}$$

Applying the associative property to (25) we obtain

$$(a_1a_2\dots a_ma_{m+1})(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1}) = (a_1a_2\dots a_m)(a_{m+1}a_{m+1}^{-1})(a_m^{-1}\dots a_1^{-1}). \tag{26}$$

Multiplying out $a_{m+1}a_{m+1}^{-1}$ in (26) we obtain

$$(a_1a_2\dots a_ma_{m+1})(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1}) = (a_1a_2\dots a_m)(a_m^{-1}\dots a_1^{-1}). \tag{27}$$

We know that

$$(a_1a_2\dots a_m)(a_m^{-1}\dots a_1^{-1}) = e \tag{28}$$

from the hypothesis of the inductive proof. Applying the transitive property of equality to (27) and (28) we obtain

$$(a_1a_2\dots a_ma_{m+1})(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1}) = e. \tag{29}$$

In a similar manner we can show that

$$(a_{m+1}^{-1}a_m^{-1}\dots a_1^{-1})(a_1a_2\dots a_ma_{m+1}) = a_{m+1}^{-1}ea_{m+1} = a_{m+1}^{-1}a_{m+1} = e.$$

From this we see can conclude that the inverse of $a_1a_2\dots a_m$ is $a_m^{-1}a_{m-1}^{-1}\dots a_1^{-1}$ for all $m \in \mathbb{Z}^+$.

□

(2) Prove that if G is a group with identity e in which $a^2 = e$ for every $a \in G$, then G is an Abelian group. Is the converse true?

Proof. Let G be a group with identity e such that $a^2 = e$ for all $a \in G$. Let $a, b \in G$. We know that

$$(ab)(ab) = e. \tag{30}$$

from the fact that G must be closed under its operation and so $ab \in G$. Multiplying a on the left side of (30) we obtain

$$a(ab)(ab) = ae. \tag{31}$$

Because e is the identity element in G we know that $ae = a$. Applying this and the transitive property of equality to (31) we obtain

$$a(ab)(ab) = a. \tag{32}$$

Applying the associative property to (32) we obtain

$$a^2b(ab) = a. \tag{33}$$

From the knowledge that $a^2 = e$, (33) becomes

$$b(ab) = a. \tag{34}$$

Multiplying b on the right side of (34) we obtain

$$b(ab)b = ab. \tag{35}$$

Applying the associative property to (35) we obtain

$$(ba)b^2 = ab. \tag{36}$$

Again, coming from the fact that any element multiplied by itself is the identity element, (36) becomes

$$ba = ab.$$

In conclusion we have shown that G is Abelian. $\square$

The converse of the statement in problem 2 is not true. For example we have the Abelian group $(\mathbb{Z}, +)$. In this group $2 + 2 \neq 0$ and so being an Abelian group does not guarantee that for every element a in the group with identity e, $a^2 = e$.