Math 31 - Homework 2 Solutions

1. [Saracino, Section 2, #1 (a), (b), (h), (i)] Which of the following are groups? Why? (That is, either verify that the axioms hold, or explain why one of them fails.)

(a) $\mathbb{R}^+$ under addition. (Here $\mathbb{R}^+$ denotes the set of all *positive* real numbers.)

(b) The set $3\mathbb{Z}$ of integers that are multiples of 3, under addition.

(c) $\mathbb{R} - \{1\}$ under the operation $a * b = a + b - ab$.

(d) $\mathbb{Z}$ under the operation $a * b = a + b - 1$.

Solution. (a) This is not a group. In particular, there is no identity, since $0 \notin \mathbb{R}^+$.

(b) This is a group. Addition clearly gives an associative operation on $3\mathbb{Z}$, and $0 \in 3\mathbb{Z}$, so it possesses an identity as well. Finally, if $a = 3m \in 3\mathbb{Z}$, then $-a = 3(-m) \in 3\mathbb{Z}$ as well, so every element has an inverse.

(c) This is a group. The operation is associative: if $a, b, c \in \mathbb{R} - \{1\}$, then

$$(a * b) * c = (a + b - ab) * c$$
$$= (a + b - ab + c) - (a + b - ab)c$$
$$= a + b + c - ab - ac - bc + abc,$$

while

$$a * (b * c) = a * (b + c - bc)$$
$$= a + b + c - bc - ab - ac - abc.$$

The identity element is 0, since

$$0 * a = a * 0 = a + 0 - a \cdot 0 = a$$

for all $a \in \mathbb{R} - \{1\}$. Finally, the inverse of an element a is $-a/(1 - a)$, since

$$a * \frac{-a}{1 - a} = a + \frac{-a}{1 - a} + \frac{a^2}{1 - a} = \frac{a - a^2}{1 - a} + \frac{-a}{1 - a} + \frac{a^2}{1 - a} = 0.$$

(d) This is also a group. The operation is associative, since if $a, b, c \in \mathbb{Z}$, then

$$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2,$$

while

$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2.$$

Also, the identity element is 1, since

$$1 * a = a * 1 = a + 1 - 1 = a$$

for all $a \in \mathbb{Z}$. Finally, given $a \in \mathbb{Z}$, the inverse is $2 - a$, since

$$a * (2 - a) = a + 2 - a - 1 = 1.$$

2. [Saracino, Section 2, #5] The following table defines a binary operation on the set $S = \{a, b, c\}$.

$*$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

Is $\langle S, * \rangle$ a group?

Solution. No, $\langle S, * \rangle$ is not a group. The identity element is a, but note that b and c do not have inverses, since there is no $x \in S$ such that $b * x = a$ or $c * x = a$.

3. [Saracino, Section 2, #8] Let G be the set of all real-valued functions f on the real line which have the property that $f(x) \neq 0$ for all $x \in \mathbb{R}$. In other words,

$$G = \{f : \mathbb{R} \to \mathbb{R} : f(x) \neq 0 \text{ for all } x \in \mathbb{R}\}.$$

Define the product $f \times g$ of two functions $f, g \in G$ by

$$(f \times g)(x) = f(x)g(x) \text{ for all } x \in \mathbb{R}.$$

With this operation, does G form a group? Prove or disprove.

Proof. G does indeed form a group. First, G is closed under $\times$, since if $f(x) \neq 0$ and $g(x) \neq 0$ for all $x \in \mathbb{R}$, then $f \times g(x) = f(x)g(x) \neq 0$ for all $x \in \mathbb{R}$. The operation $\times$ is associative, since multiplication of real numbers is associative: for all $x \in \mathbb{R}$, we have

$$(f \times g) \times h(x) = (f \times g)(x)h(x) = (f(x)g(x))h(x) = f(x)(g(x)h(x)) = f \times (g \times h)(x),$$

so $(f \times g) \times h = f \times (g \times h)$ for all $f, g, h \in G$. The identity is given by the constant function $\mathbf{1} : \mathbb{R} \to \mathbb{R}$, where $\mathbf{1}(x) = 1$ for all $x \in \mathbb{R}$, since

$$f \times \mathbf{1}(x) = f(x) \times \mathbf{1}(x) = f(x) \cdot 1 = f(x)$$

and similarly $\mathbf{1} \times f(x) = f(x)$ for all $x \in \mathbb{R}$. Finally, if $f \in G$, then the function $f^{-1}(x) = 1/f(x)$ (note that this does not mean the inverse function, just the reciprocal) exists (since $f(x) \neq 0$ for all x) and lies in G, so

$$f \times f^{-1}(x) = f(x) \cdot \frac{1}{f(x)} = 1 = \mathbf{1}(x)$$

for all $x \in \mathbb{R}$. Therefore, G is a group. $\qquad\square$

6. If G is a group in which $a * a = e$ for all $a \in G$, show that G is abelian.

Proof. To show that G is abelian, we need to show that for any $a, b \in G$, $ab = ba$. Let $a, b \in G$; then $a^2 = e$ and $b^2 = e$. Also, we have $(ab)^2 = e$, so we can compute as follows:

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

Using associativity to regroup, we have

$$(aa)(ba)(bb) = a^2(ba)b^2 = e(ba)e = ba.$$

Therefore, $ab = ba$. Since a and b were arbitrary elements of G, we have shown that G is abelian. $\quad\square$

Extra credit: We saw in class that any group of order 1, 2, or 3 is abelian. Show that any group of order 4 must be abelian. [Hint: Try to write down all the possible group tables in this case. Up to reordering the elements of the group, there will only be two possibilities.]

Proof. To do this, we'll write down the possible group tables for a group of order 4. We claim that there are only 2 possibilities. Suppose that G is a group of order 4, and write the elements as

$$G = \{e, a, b, c\},$$

where e represents the identity. Each of the three nonidentity elements must have an inverse, and there are two ways to do this. We can either pair off two of the elements to be inverses of each other, while the third is its own inverse, say

$$a^2 = e$$
$$bc = e$$

The other option is to make all three elements equal to their own inverses, i.e.,

$$a^2 = b^2 = c^2 = e.$$

In the first case, let's assume that $a = a^{-1}$, or $a^2 = e$. Then we must have $ab = c$ and $ac = b$. (We can't have $ab = b$, since this would imply that $a = e$, which we are assuming is not the case.) Similarly, we'll have to have $ba = c$ and $ca = b$. In this case the group table looks like:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

In the second case, we assume that a, b, and c all square to e. As before, we must have $ab = c$, $ac = b$, $ba = c$, and $ca = b$. The only things left to deal with are bc and cb. These must both equal a (since we can't have $bc = b$ or $bc = c$, etc.), so the group table looks like:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

In either case, it is easy to check via the table that the group in question is abelian. [Note: There are actually other possible group tables. In the first case we made a choice regarding which element would square to e, and we chose a. By choosing either $b^2 = e$ or $c^2 = e$, we could have written down two slightly different group tables. However, they can both be obtained from the one we wrote down by simply rearranging the group elements.]   □

Extra extra credit: Try to extend the extra credit problem by showing that any group of order 5 must also be abelian.

Proof. Let G be a group of order 5, and suppose to the contrary that G is nonabelian. Then there are two elements $a, b \in G$ which do not commute. Then e, a, b, ab, and ba are all distinct elements of G, and since G has only five elements, these are all the elements of G. We claim that a^2 is not on this list. If $a^2 = e$, then we have

$$a * e = a$$
$$a * a = e$$
$$a * b = ab$$
$$a * (ab) = a^2 b = b$$

and by process of elimination,
$$a * (ba) = ba.$$

However, this last equation forces $a = e$, which is absurd. Next, $a^2 \neq a$, since this would also imply that $a = e$. If $a^2 = b$, then a and b would commute, which we have assumed is not the case. Finally, if either $a^2 = ab$ or $a^2 = ba$, then $a = b$, which is again absurd. Therefore, we have produced a sixth distinct element of G, which only has five elements. This is a contradiction, and since the only thing we have assumed is that G is nonabelian, it must be the case that any group G with $|G| = 5$ is abelian. $\qquad\square$